HX2 Reference Guide

LXE | **FLEX** | **Wearable Computer**

E-EQ-HX2RG-M

Notices

LXE Inc. reserves the right to make improvements or changes to published HX2 information at any time without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, LXE assumes no liability resulting from any errors or omissions in this publication, or from the use of the information contained herein. Further, LXE Incorporated, reserves the right to revise this publication and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

Trademarks

LXE® and **Spire**® are registered trademarks of LXE Inc.

RFTerm® is a registered trademark of EMS Technologies, Norcross, GA. EMS is now part of Honeywell.

Microsoft®, ActiveSync®, MSN, Outlook®, Windows®, Windows Mobile®, the Windows logo, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Intel and Intel XScale are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Summit Data Communications, Inc. Summit Data Communications, the Summit logo, and “The Pinnacle of Performance” are trademarks of Summit Data Communications, Inc.

Java® and Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. or other countries, and are used under license.

The **Bluetooth**® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by LXE, Inc. is under license.

PowerScan is a registered trademark of Datalogic Scanning, Inc., located in Eugene, OR.

Symbol® is a registered trademark of Symbol Technologies. **MOTOROLA**® and the Stylized M Logo are registered trademarks of Motorola®, Inc.

Wavelink®, the Wavelink logo and tagline, Wavelink Studio™, Avalanche Management Console™, Mobile Manager™, and Mobile Manager Enterprise™ are trademarks of Wavelink Corporation, Kirkland.

When any part of this publication is in PDF format: “Acrobat ® Reader Copyright © 2011 **Adobe** Systems Incorporated. All rights reserved. Adobe, the Adobe logo, Acrobat, and the Acrobat logo are trademarks of Adobe Systems Incorporated” applies.

Other product names mentioned within this publication may be trademarks or registered trademarks of other companies.

Table of Contents

Introduction

The LXE® HX2 is a small, lightweight mobile computer designed to be worn on a person's arm or waist. The HX2 is most useful for applications that require computational support while the user's hands are actively engaged with the physical environment, including piece picking to carts, containers or conveyers; case picking; parcel moves; and broken case activities.

End User License Agreement (EULA)

When a new HX2 starts up a EULA is displayed on the touchscreen. It remains on the screen until the Accept or Decline button is tapped with a stylus.

Tap the Accept button to accept the EULA terms and the HX2 continues the startup process. The EULA is not presented to the user again.

Tap the Decline button to decline the EULA and the HX2 will reboot. It will continue to reboot until the Accept button is tapped with the stylus.

Note: The EULA will be presented after any operating system upgrade or re-installation, including language-specific operating systems.

Important Battery Information

Note: Backup Battery -- If the HX2 has been without a power source (connected to a fully charged tethered battery or docked in a powered cradle) for an extended period of time or if HX2 external power sources become completely discharged or dead, a fully charged backup battery will last for up to 15 minutes. If the backup battery is fully discharged, the HX2will reset as soon as it is docked in a powered cradle or connected to a fully charged tethered battery. A reset will cause loss of data and custom programs in RAM. Always store unused HX2s with a fully charged tethered battery. If possible, ensure the HX2 is periodically docked in a powered cradle to maintain an optimum backup battery charged status.

To check battery status, tap **Start | Settings | Control Panel | Battery** tab.

- Until the tethered battery and backup battery are completely depleted, the HX2 is always drawing power from the batteries (On).
- New Standard / Extended batteries must be fully charged prior to use.
- Whenever possible, place the HX2 in a powered cradle to conserve tethered battery power and recharge the backup battery.
- When a new battery is tethered to the HX2 for the first time (or after the backup battery is depleted), the Time and Date reverts to factory default values.
- Backup battery replacement is performed by LXE.

The HX2 cradle can charge two standard batteries in less than four hours or two extended batteries in less than 8 hours in the battery wells behind the HX2 docking bay. The cradle requires an external power source before battery charging can occur.

The HX2 Multi-Charger can charge up to six batteries at the same time. Each charging bay can accept either type of battery. The Multi-Charger requires an external power source before charging/analyzing can occur.

Li-Ion Battery

When disposing of the tethered batteries, the following precautions should be observed: The battery should be disposed of properly. The battery should not be disassembled or crushed. The battery should not be heated above 212°F (100°C) or incinerated.

Continuous Scan Mode

Start | Settings | Control Panel | Scanner | Barcode Tab

Enabling Continuous Scan Mode will ensure the laser is always on and decoding.

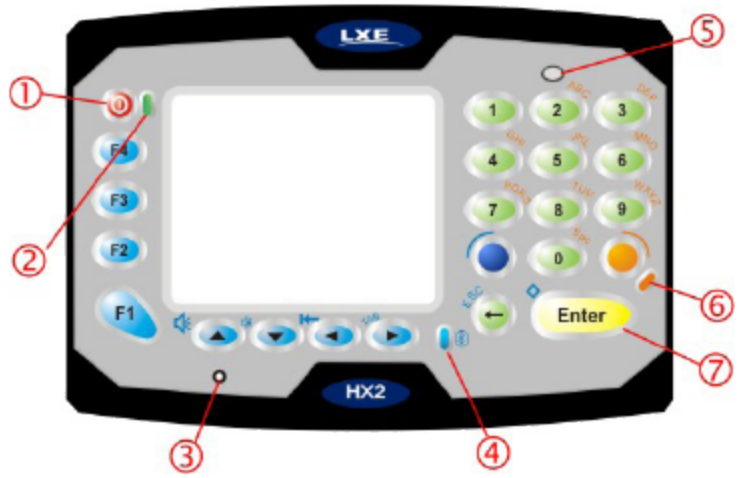
Caution: Laser beam is emitted continuously. Do not stare into the laser beam.

Components

Front

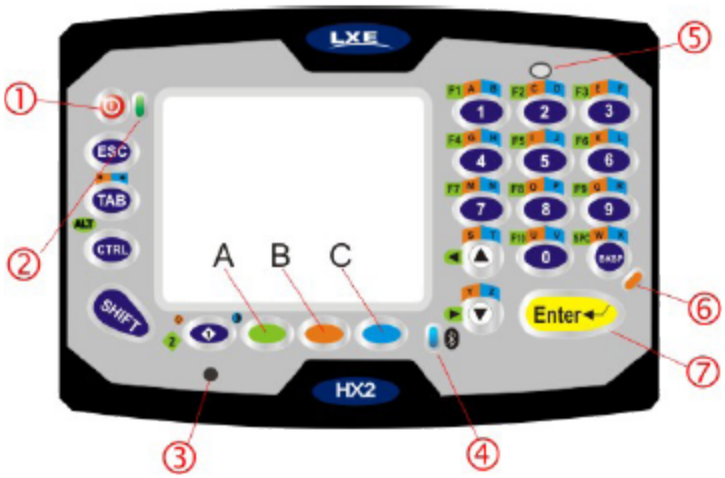
Note: Alpha Mode LED is not used with the Dual Alpha Keypad and the Triple Tap Keypad.

Alpha Mode 3 Tap Keypad



1. On / Off Button
2. System Status LED
3. Microphone
4. Bluetooth LED
5. Speaker
6. Alpha Mode LED
7. Enter Button

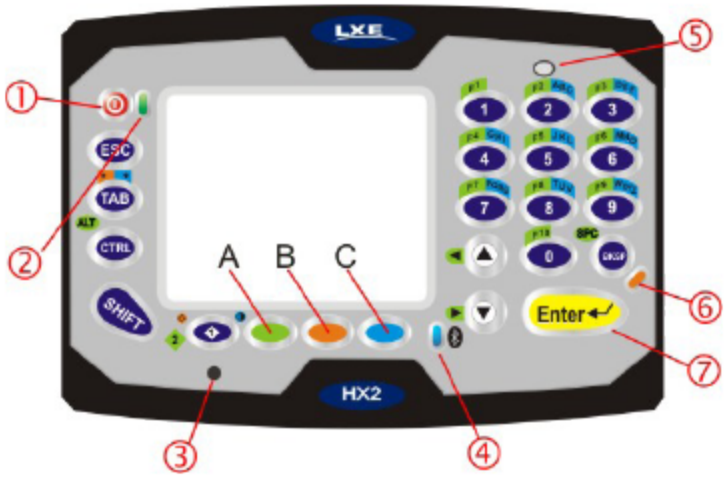
Dual Alpha Keypad



1. On / Off Button
2. System Status LED
3. Microphone
4. Bluetooth LED
5. Speaker
6. Alpha Mode LED
7. Enter Button

A. Green Button
B. Orange Button
C. Blue Button

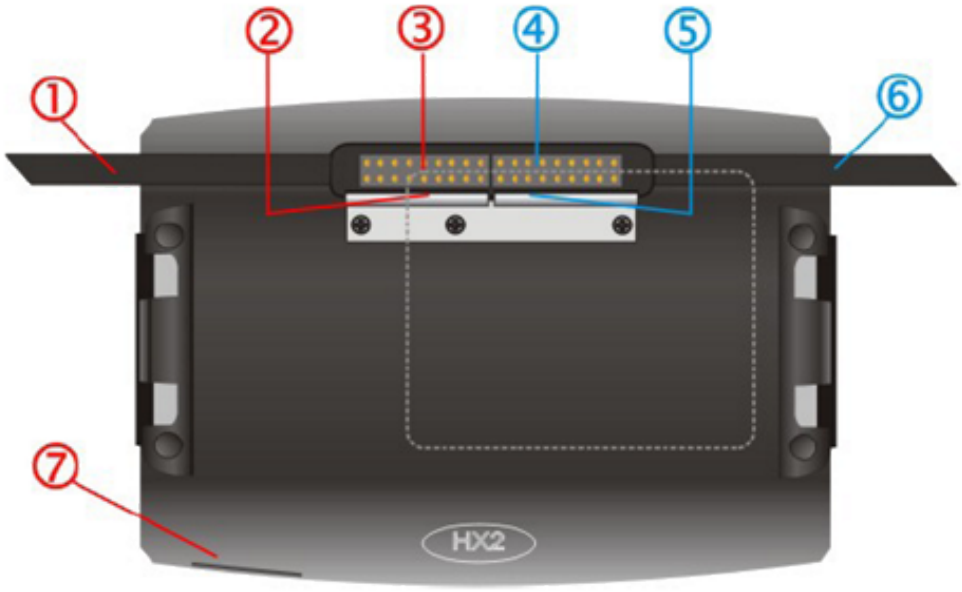
Triple Tap Keypad



1. On / Off Button
2. System Status LED
3. Microphone
4. Bluetooth LED
5. Speaker
6. Alpha Mode LED
7. Enter Button

A. Green Button
B. Orange Button
C. Blue Button

Back



Wear on Left Side, Ring on Left Hand	Wear on Right Side, Ring on Right Hand
1. Ring Scanner Tether cable channel 2. Retaining Clip for Ring Scanner Tether Connector 3. Ring Scanner cable connector 4. Battery Cable connector 5. Retaining Clip for Tethered Battery Connector 6. Tethered Battery Cable channel 7. Cradle Connector	1. Tethered Battery Cable channel 2. Retaining Clip for Tethered Battery Connector 3. Battery Cable connector 4. Ring Scanner cable connector 5. Retaining Clip for Ring Scanner Tether Connector 6. Ring Scanner Tether cable channel 7. Cradle Connector

Connectors

Ring Scanner / Audio / Battery Connection

Connector 1 is on the left.

Connector 2 is on the right.

Both connect to cables for:

- Tethered Ring Scanner (Laser or Imager)
- Tethered Headset / Microphone and Battery
- Tethered Battery

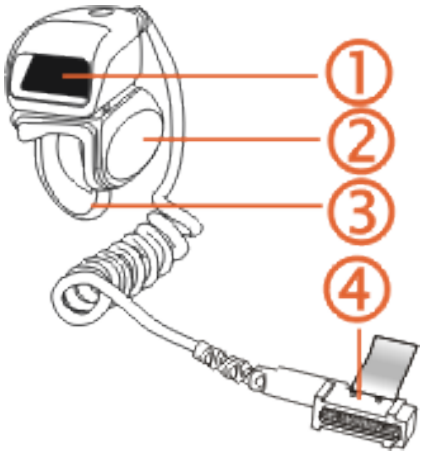
Cradle Connection

Connector 3 is at the base of the HX2. It connects to the Cradle. When the HX2 is in a powered cradle, the HX2 receives external power through the Cradle connector.

USB Keyboard or USB Mouse input is received through the Cradle connector when the HX2 is in a cradle.

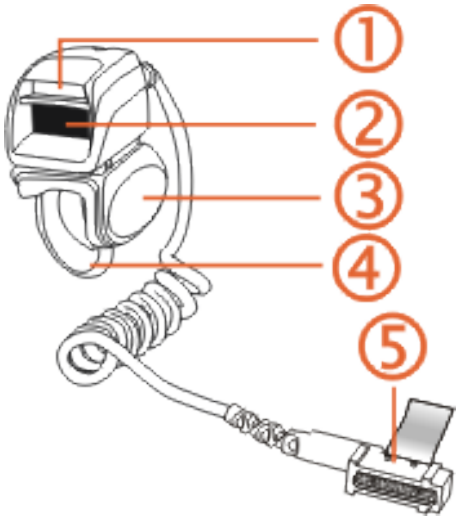
Ring Scanner and Ring Imager

The trigger module and ring strap module are user replaceable.



1. Scan Window
2. Trigger
3. Ring Strap
4. Connector

Laser Scanner

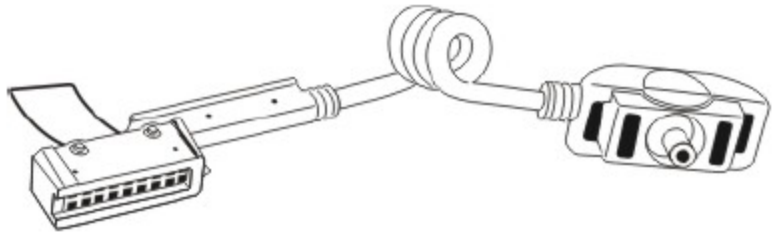


1. Illumination LEDs
2. Scan Window
3. Trigger
4. Ring Strap
5. Connector

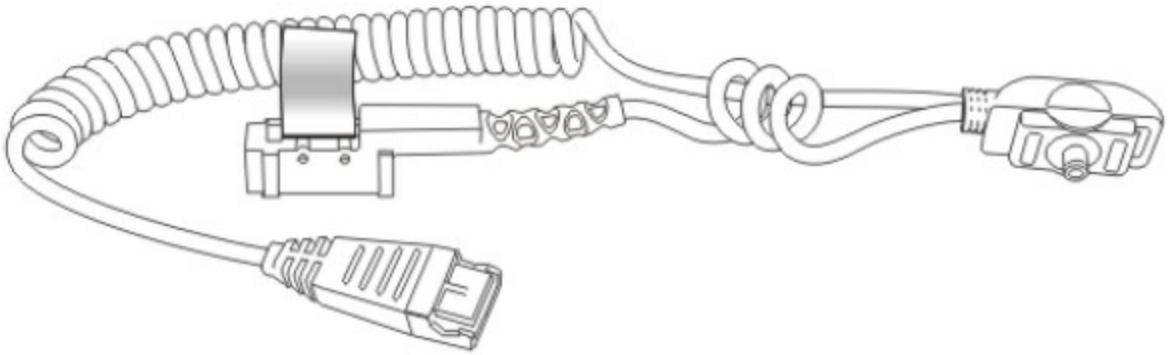
Laser Imager

Cables

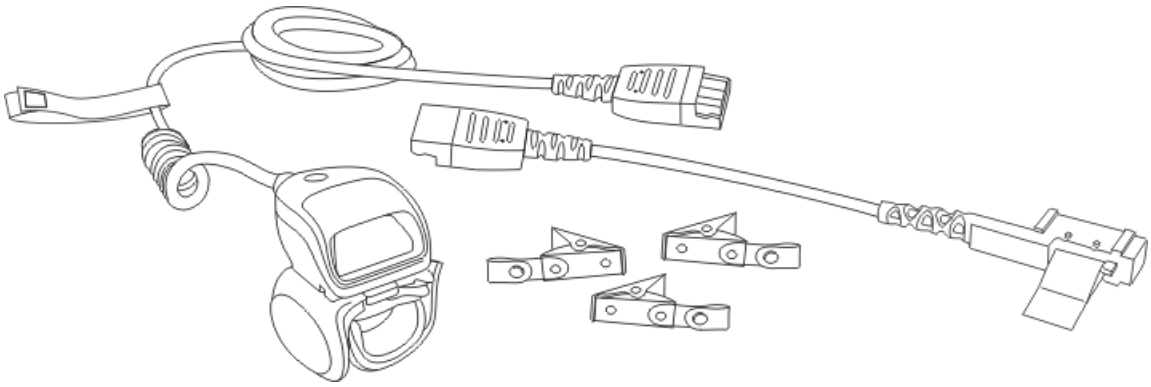
Battery and HX2 Connector



Audio, Battery and HX2 Connector



Ring Scanner Extended Cable



Li-Ion Battery

Main battery charging is handled exclusively by the HX2 Multi-Charger/analyzer and the battery charger integrated into a powered HX2 cradle.

The Standard battery is much thinner than the Extended battery.

Each battery will fit in the battery sleeve on an armband, hip flip and the voice case.

Note: Do not allow water or chemical cleaning agents of any kind to come in contact with the battery charging contacts or the battery cable connector; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Battery Connectors

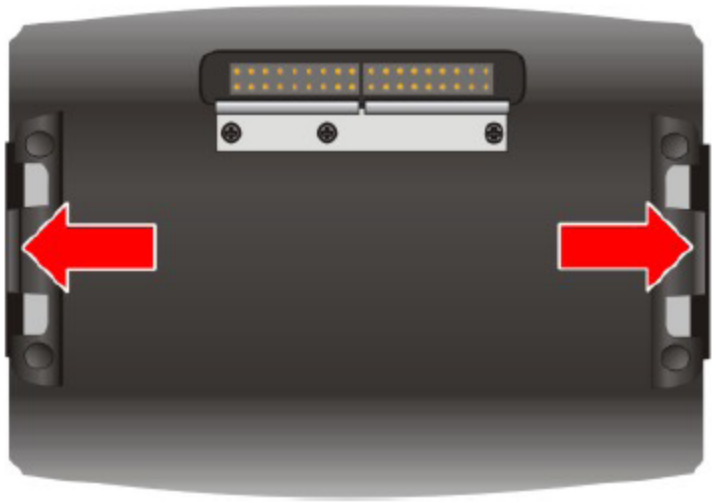
Note: When placing the tethered battery in an armband or hip flip battery sleeve, ensure the Battery Charge/Connect terminals are protected from accidental damage by keeping them covered by the sleeve fabric at all times.

Standard Battery

Extended Battery

Mounting Bracket Clips

Mounting brackets are pre-installed to the back of the HX2. The brackets (one on each side) secure the HX2 to the mounting bracket clips on a hip flip or the armband.

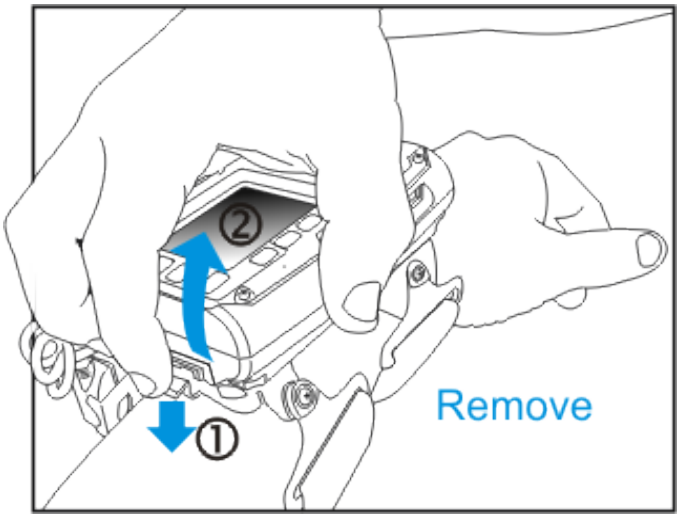


Connect

Center the HX2 over the mount assembly and gently push down until both mount bracket clips snap over the brackets on the HX2. Carefully test the connection to make sure the HX2 is secured to the armband or hip flip.

Reset the connection by pressing down on either mounting clip to release the HX2 and try again.

Disconnect



1. Push down on bracket clip
2. Pull up at a 45 degree angle

Remove the HX2 from the mount assembly by pushing down on either mounting clip, or both, until the HX2 mounting bracket disconnects.

Or you can disconnect from one clip, then lift the HX2 up at a 45 degree angle until the other side disconnects. Lift the HX2 up and away from the mount assembly.

System Status LEDs

When multiple system status conditions are present, the most urgent condition is indicated. The conditions listed below are in increasing order of urgency by LED type.

	LED	Color - Activity	Indicates ...
1	System Status	Green - Blinking	Display turned off when timer expires. This will help to conserve battery power. Tap the screen or press any key (except the Power button) to turn the display on again. The HX2 is not in Suspend Mode.
		Red - Steady	Main Battery Low. If the main battery is not replaced with a fully charged battery before the main battery fails, the HX2 is turned Off.
		Red - Blinking	Main Battery Power Fail
		Off	Suspend Mode
2	Bluetooth	Blue - Blinking Slowly	Bluetooth is active but not connected to a device.
		Blue – Blinking Medium	Bluetooth is paired and connected to a device.
		Blue - Blinking Fast	Bluetooth is discovering nearby Bluetooth devices.
		Off	Bluetooth hardware has been turned off or does not exist in the HX2.
3	Alpha	Amber - Steady	Amber mode enabled (Alpha key not used with Dual Alpha keypad and the Triple Tap keypad.)

Reboot

When the Windows CE desktop is displayed or an application begins, the power up (or reboot) sequence is complete.

Warm Boot

Start | Run

A warm boot function does not affect the operating system, but data and programs in RAM are cleared, and registry changes, if any, are saved. Network and Bluetooth connections will need to be re-established.

Tap **Start | Run** and type WARMBOOT.EXE or WARMBOOT. This command is not case-sensitive.[1] Tap the OK button. This process takes less than 15 seconds. Temporary data not saved is lost.

Note: There may be slight delays while the wireless client connects to the network, re-authorization for voice-enabled applications completes, Wavelink Avalanche management of the HX2 startup completes, or Bluetooth relationships establish or re-establish.

Cold Boot

Start | Run

The Cold Boot function reboots the device, erases all registry data, and user-specified settings. The factory default settings are restored when the HX2 powers on again.

Tap **Start | Run** and type COLDBOOT.EXE or COLDBOOT. This command is not case-sensitive. Tap the OK button.

Note: Because of the extreme nature of cold boot, LXE recommends using this command only as an emergency (or when instructed to do so as part of a specific HX2 procedure).

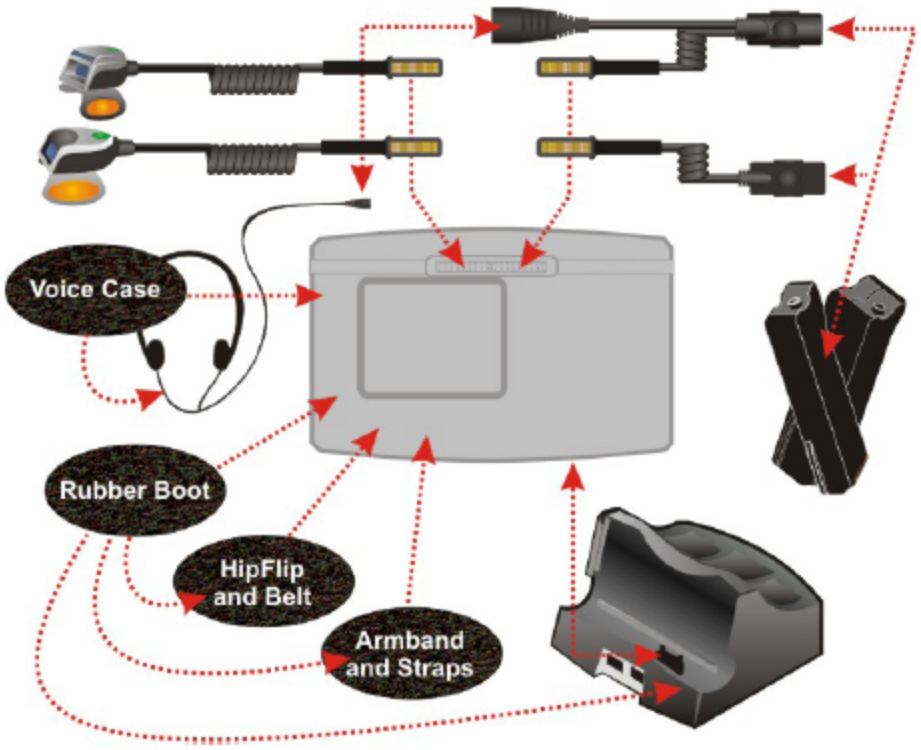
HX2 Troubleshooting

Can't change the date/time or adjust the volume.	AppLock is installed and may be running in User Mode on the HX2. AppLock user mode restricts access to the control panels.
Touchscreen is not accepting stylus taps or needs recalibration.	Press <Ctrl>+<Esc> to force the Start Menu to appear. Use the tab, backtab and arrow keys to move the cursor from element to element.
HX2 seems to lockup as soon as it is warm booted.	There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, and Bluetooth relationships establish or re-establish. When the desktop appears or an application begins, the HX2 is ready for use.
New HX2 main batteries don't last more than a few hours.	New batteries must be fully charged prior to first use. Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the HX2 is always 'on' even when in the Suspend state and draws a small amount of battery power at all times.
Keep losing ActiveSync connection between my host computer and the HX2.	When the HX2 enters Suspend Mode, all connections are closed to save battery power. When the HX2 wakes up, if ActiveSync connection does not automatically re-establish, disconnect the cable, wait 1-2 seconds and reconnect the cable.

[1] The text typed in the text box can be upper or lower case or a combination of upper and lower case letters.

Hardware

System Hardware



802.11b/g and a/b/g Wireless Client

The HX2 has an LXE 802.11x network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. Adjusting power management on the network card is set to static dynamic control.

WEP, WPA and LEAP are supported.

Central Processing Unit

The CPU is a 400MHz Intel Xscale PXA255 CPU. The operating system is Microsoft® Windows® CE 5. The OS image is stored on an internal SD flash card and is loaded into DRAM for execution.

Xscale turbo mode switching is supported and turned on by default.

The HX2 supports the following I/O components of the core logic:

- One SD card slot, inaccessible to the end-user.
- One TTL serial port designed to interface with LXE ring scanner only.
- One RS-232 serial port accessible via the cradle.
- USB master accessible via the cradle.
- USB client accessible via the cradle.
- One Digitizer Input port (Touch screen).

System Memory

The 400MHz CPU configuration supports 128MB SDRAM, 128MB SD card. SD card location is inaccessible to the end user.

The system optimizes for the amount of SDRAM available. The operating system executes out of RAM.

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup. The UUID required by CE 5.0 is stored in the boot flash. A second copy of the bootloader code is stored on the internal SD Flash drive, so that if a damaged bootloader is detected, it may be re-flashed correctly.

Internal SD Memory Card

The HX2 has one SD card interface for storage of operating system and program code, as well as persistent storage. The SD slot is inaccessible and ships with an LXE-qualified 128MB (optional 512MB) SD Flash card.

The internal SD flash card supports a FAT file system, via a special device driver, and appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface. Operating system files are hidden on this drive with a terminal unique identifier in the internal flash, to prevent them being accidentally erased by a user. In addition, the registry hive files are stored on this device. The amount of Flash memory available for customer use is the original SD flash card size less 40MB.

Video Subsystem

The QVGA touchscreen is a 2.5" (6.3 cm) diagonal viewing area, 320 by 240 pixel Transflective Active Color LCD. The turn-off timing is configured through the Start | Settings | Control Panel | Display | Backlight icon. The display controller supports Microsoft CE 5.0 graphics modes.

A touchscreen allows mouse functions (tapping on the display or signature capture) using an LXE approved stylus. The touchscreen has an actuation force with finger less than 100 grams.

The color display has an LED backlight and is optimized for indoor use. The display appears black when the mobile device is in Suspend Mode.

Power Supply

The LXE HX2 uses two batteries for operation. A Lithium-Ion (Li-Ion) battery supplies power to the HX2 only when tethered to the HX2. The main battery is either the 2000 mAh (Standard) or the 4000 mAh (Extended) battery. Only one main battery can be tethered to the HX2 at a time. The batteries can be hot-swapped after the HX2 is placed in Suspend mode.

The internal backup battery is a 50 mAh Nickel Cadmium (NiCad) battery. The backup battery is recharged indirectly by the HX2 with a tethered battery. Recharging maintains the backup battery near full charge at all times. When the backup battery is fully drained, it may take up to 5 hours to recharge. The capability to discharge the backup battery is provided (Start | Settings | Control Panel | Battery) to allow the user to condition the backup battery in order to recover full battery capacity. The backup battery must be replaced by qualified service personnel. The backup battery has a minimum 2 year service life.

When the HX2 is docked in a powered cradle, the HX2 receives USB/serial signals through the cradle connector on the bottom of the HX2 and the cradle connector in the HX2 docking bay. The HX2 must be firmly seated in the docking bay before USB/serial communication can occur. An extra standard or extended Li-Ion battery pack can be recharged in the powered cradle while one of the batteries is tethered to, and powering, the HX2. The standard battery is fully recharged in a powered cradle in 4 hours. The extended battery is fully recharged in 8 hours.

*Note: **Docked HX2** -- An uninterrupted external power source (wall AC/DC adapter connected to the HX2 cradle) transfers signals from the USB ports in the front of the cradle and the serial port on the back of the cradle, to the HX2. HX2 frequent connection to a fully charged tethered battery, is recommended to maintain backup battery charge status, as the backup battery cannot be recharged by a dead or missing tethered battery.*

The LXE HX2 Battery Charger is designed to simultaneously charge up to six standard HX2Rechargeable Lithium Ion Battery Packs in less than four hours, depending upon battery pack temperature and ambient conditions. The Extended battery

packs require less than 8 hours. The HX2 Multi-Charger can charge up to five Standard and Extended batteries when they are not tethered to the HX2.

Bluetooth LXEZ Pairing

The HX2 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains wireless connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections to from the HX2. However, the HX2 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the HX2 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

The Bluetooth client can simultaneously connect to one Bluetooth scanner and one Bluetooth printer. Up to four Bluetooth devices can be paired and managed using a control panel (Start | Settings | Control Panel | Bluetooth).

Blue LED	Blinking slowly	Bluetooth is active but not connected to a device.
Blue LED	Blinking medium	Bluetooth is paired and connected to a device.
Blue LED	Blinking fast	Bluetooth is discovering other Bluetooth devices.
Blue LED	Unlit	Bluetooth hardware has been turned off or does not exist in the HX2.

Barcode data captured by the Bluetooth scanner is manipulated by the settings in the HX2 Scanner Properties control panel.

Multiple beeps may be heard during a barcode scan using a mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the barcode data is accepted/rejected, and other beeps from the HX2 during final barcode data manipulation.

Input/Output Connectors

The HX2 has three I/O connectors. Two connectors are located next to each other on the back of the mobile device. Each of the two connectors (one for left-handed users and the other for righthanded users) interfaces with peripherals such as a Laser Ring Scanner, an Imager Ring Scanner, an audio headset and a tethered battery.

Connector 1 and Connector 2 are located on the back of HX2 and each connector can accommodate a:

- Tethered Laser or Imager Scanner
- Tethered Headset/Microphone and HX2 Battery
- Tethered Battery

Connector 3 Located on the bottom of HX2 and can accommodate:

- Cradle
- Cradle Power Input
- USB Keyboard and mouse through cradle

The third I/O connector is used when docking the HX2 in a cradle. The cradle has RS-232, USB Client, unpowered USB Host and Power connections. The power connection on the cradle supplies power to the battery charging bays. All communication is managed by the cradle.

Audio Support

Speaker

The internal speaker supplies audible verification signals normally used by the Window's CE operating system. The speaker is located on the front of the HX2, above the [2] key. The mobile device emits a Sound Pressure Level (loudness) of at least 102 dB measured as follows:

- Frequency: 2650 + 100 Hz
- Distance: 10 cm on axis in front of Speaker opening in front of unit.
- Duration : Continuous 2650 Hz tone.

The default is 1 beep for a good scan and 2 beeps for a bad scan.

Volume Control

Volume control is managed by a Windows CE control panel applet, an API and key sequences. To adjust speaker volume use the:

- Blue+Up Arrow and Blue+Down Arrow keys on the Alpha Mode 3 Tap keypad
- Orange+Diamond 1+Up Arrow and Orange+Diamond 1+Down Arrow keys on the Dual Alpha and Triple Tap keypads.

Volume control is covered in greater detail later in this guide.

Voice

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset connected to the "Tethered Headset/Microphone and HX2 Battery" accessory cable.

Touchscreen

The VGA display with touchscreen is an active TFT color unit capable of supporting VGA graphics modes at 50 dpi or greater. Display size is 320 x 240 pixels in landscape orientation; the diagonal viewing area is 2.5 inches (6.3 cm). The covering is designed to resist stains and has an anti-glare and anti-reflective coating. The touchscreen allows signature capture and touch input. The touchscreen responds to an actuation force (touch) of 4 oz. of pressure (or less).

The color display is optimized for indoor lighting. The LED backlight can be adjusted using the arrow keys. The display is black when the device is in suspend mode or when both batteries have expired and the unit is Off.

Touchscreen protective film is available from LXE.

Keypads

There are three keypads available: the Alpha Mode 3 Tap, the Dual Alpha and the Triple Tap. Use the Input Panel to enter special keys. Assign CE functions using Mappable Keys.

The Alpha Mode 3 Tap Keypad

The Alpha and Blue keys do not auto-repeat. Default timeout for any pressed key in any mode is 0.15 second.

Alpha Modifier Key

Tap **Start | Settings | Control Panel | KeyPad Control Panel** icon.

Persistent – By default, the Alpha key is persistent. Disable the radio button to disable Alpha key persistence. The Alpha mode LED is turned on when the Alpha mode is on.

When Persistent is enabled, the behavior of the Alpha modifier key is as follows:

- Pressing the Alpha key once toggles the Alpha mode and the orange LED illuminates.
- Pressing the Alpha key twice quickly (roughly twice in half a second) sets the Alpha mode and enables upper case (regardless of the previous state of the Alpha key). The orange LED illuminates.

If Alpha persistence is set to Off, the orange LED is off and Alpha mode is exited when a different key is pressed. Pressing the Blue key modifier On or Off does not change the state of the Alpha mode. The Alpha key does not need to be held down when another key is pressed.

When the Alpha key is kept pressed down while another key is pressed, then the Alpha mode is considered On (therefore the Alpha LED will turn on when the button is pressed, not when it is released). In this case, the Alpha mode is exited when the user releases the Alpha key, no matter if persistence is set to On or Off.

On the fourth (or fifth for the 7 and 9 keys) keyclick using a number key, in Alpha mode, the result is the specific number.

Blue Modifier Key

Pressing the Blue key once toggles the Blue mode. The Blue mode is exited when a key is pressed (including the Alpha key).

The Blue key does not need to be held down when another key is pressed.

When the Blue key is kept pressed down while another key is pressed, then the Blue mode is considered On. In this case, the Blue mode is exited when the user releases the Blue key. .

Mappable Keys

Tap **Start | Settings | Control Panel | KeyPad Control Panel** icon.

There are 29 key combinations that can be mapped using the KeyPad Control applet.

Key functions shown below (available on most 101-key keyboards) can be mapped to any of the 29 key combinations.

- CTRL
- ALT
- DELete
- Function Keys F9 and F20
- Insert
- Shift
- Print Screen
- SysRq
- Scroll Lock
- Pause
- NumLock
- Home
- PageUp
- PageDown
- End

Use the **Input Panel** to insert the following characters:

< > { } [ ] ( ) _ + : ; “ ‘ ? / ~ ` ! @ # $ % ^ & |

The mappable keys can be mapped by the user to generate any key code defined by Windows CE.

The Dual Alpha Keypad

The Dual Alpha keypad is set as the default keypad when the Dual Alpha or Triple Tap keypad has been shipped.

Features

- The Dual Alpha keypad modifier keys are the Green, Orange, Blue, Shift and Control (CTRL) keys.
- Modifier keys are sticky keys. Any modifier key pressed after itself toggles the specific modifier key off.
- Alpha keys are accessed by two taps: a modifier key and a number key.
- Orange Alpha LED near the Backspace key has no function on this keypad. • Any key press exits volume control mode. Any key press exits backlight control mode.
- F1 through F10 function keys are available using the keypad. Function keys F11 through F24 require multiple key-presses.
- Keys can be mapped by the user to generate any key code defined by Windows CE.
- Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

Note: The keypad is installed and activated by LXE prior to shipment. Contact LXE Customer Support for assistance.

The Triple Tap Keypad

Requires file activation to setup the Triple Tap keypad for daily use. Setup requires the Use Triple Tap Keypad checkbox be checked in the HX2 Options Control Panel. Tap OK.

Features

The modifier keys are the Green, Orange, Blue, Shift and Control (CTRL) keys.

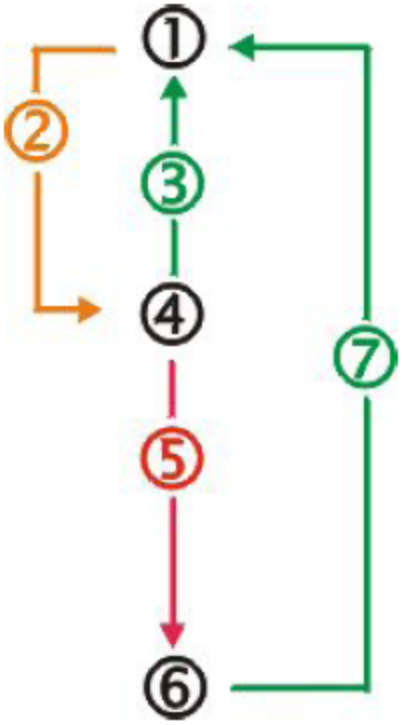
- Modifier keys are sticky keys. Any modifier key pressed after itself toggles the specific modifier key off.
- Alpha keys are accessed by several taps: the blue modifier key and one to four taps of a number key. Capital keys also require a Shift key tap.
- The orange Alpha LED has no function on this keypad and is off. • The default timeout for any Alpha key is 0.15 second.
- Any key press exits volume control mode. Any key press exits backlight control mode.
- F1 through F10 function keys are available using the keypad. Function keys F11 through F24 require multiple key-presses.
- Keys can be mapped by the user to generate any key code defined by Windows CE.
- Use Start | Settings | Control Panel | Keypad | KeyMap tab to change the Diamond 1 and Diamond 2 key keypress defaults.

The alphabet characters wrap for keys 2 – 9, for example:

- Blue + 2 produces a lower case a
- Blue + 22 produces a lower case b
- Blue + 222 produces a lower case c
- Blue + 2222 produces the number 2

Power

Power Modes



1. **On**
2. Tap Power key or Suspend timer has timed out
3. Power key, any key, scan button tap, or touch screen tap
4. **Suspend**
5. Tethered battery and backup battery depleted
6. **Off**
7. Power Restored and On key pressed

Primary Events Listing

- Any key on the keypad
- COM1 activity
- Stylus touch on the touch screen
- Docked in powered cradle
- Power button tap
- Bluetooth device reconnect / disconnect message
- Ring scanner activity

On Mode

The Display

When the display is On:

- the keypad, touchscreen and all peripherals function normally
- the display backlight is on until the Backlight timer expires

The HX2

After a new HX2 has been received, a charged battery tethered, and the Power key tapped, the HX2 is always On until both batteries are drained completely of power.

When the tethered battery and backup battery are drained completely, the unit is in the Off mode. The unit transitions from the Off mode to the On mode when a charged battery is attached to the tether or external power is applied (for example, by docking the HX2 in a powered cradle) and the HX2 Power key is pressed.

Suspend Mode

The HX2

The Suspend mode is entered when the unit is inactive for a predetermined period of time or the user taps the Power key.

HX2 Suspend timers are set using Start | Settings | Control Panel | Power | Schemes tab.

Wake up Events - all configurable via an LXE Power Management API call:

- Any key on the keypad
- Stylus touch on the touchscreen
- Scan button on ring scanner pressed
- Docked in a powered cradle
- Power button tap

When the unit wakes up, the Display Backlight and the Power Off timers begin the countdown again. When any one of the above events occurs prior to the Power Off timer expiring, the timer starts the countdown again.

The HX2 should be placed in Suspend Mode before hotswapping the main battery.

Hotswapping the Ring Scanner does not require placing the HX2 in Suspend Mode.

Off Mode

The unit is in Off Mode when the tethered battery and the backup battery are depleted. Connect a fully charged main battery and press the Power key to turn the HX2 On.

Batteries

The HX2 is designed to work with a Lithium-Ion (Li-ion) tethered battery from LXE. Under normal conditions it should last approximately eight to ten hours before requiring a recharge. The more you use the ring scanner or the wireless transmitter, the shorter the time required between battery recharges.

A suspended HX2 maintains the date and time for a minimum of two days while tethered to a battery that has reached the Low Warning point and a fully charged backup battery. The HX2retains data, during a battery hot swap, for at least 5 minutes.

Note: New battery packs must be charged prior to use. The Standard batteries require less than four hours and the Extended batteries require less than 8 hours.

Checking Battery Status

Tap the **Start | Settings | Control Panel | Power | Battery** tab. Battery level, power status and charge remaining is displayed. Turbo setting is enabled/disabled using this applet.

Note: Battery power drain increases substantially in Turbo mode.

Status LED and the Batteries

When the LED is . . .	The Status is . . .	Comment
Blinking Red	Main Battery Power Fail	Replace the main battery with a fully charged main battery.
Steady Red	Main Battery Low	Low Battery Warning. If the main battery is not replaced with a fully charged battery before the main battery fails, the HX2 is turned Off.
No Color	Good	No user intervention required.

Main Battery Pack

The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the HX2 MultiCharger, HX2 Cradle or the HX2 unit.

Whenever possible, protect the battery charging terminals (five small round circles) by keeping them covered by the battery sleeve fabric. The battery pack is resistant to impact damage.

Under normal conditions a properly tethered Standard battery should last a minimum of approximately eight hours before requiring a recharge, the Extended battery a minimum of approximately 16 hours.

Battery Hotswapping

Important: When the backup battery power is Low or Very Low (Start | Settings | Control Panel | Power | Battery tab) dock the HX2 in a powered docking cradle before replacing the battery pack.

When the main battery power level is low, the HX2 will signal the user with the low battery warning indicator (the Status LED remains a steady red) that continues until the main battery is replaced, the battery completely depletes, or external power is applied to the HX2 using a powered cradle.

You can replace the main battery by first placing the device in Suspend Mode then removing the discharged main battery and tethering a charged main battery within a five minute time limit (or before the backup battery depletes).

When the main battery is disconnected the device enters Critical Suspend state, the HX2 remains in Suspend mode, the display is turned off and the backup battery continues to power the unit for at least five minutes. Though data is retained, the HX2 cannot be used until a charged main battery pack is connected. After tethering the full battery, press the Power key.

Full operational recovery from Suspend can take several seconds while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the HX2 startup completes, and Bluetooth relationships establish or reestablish.

If the backup battery depletes before a fully charged main battery can be inserted, the HX2 will turn Off.

Low Battery Warning

It is recommended that the main battery pack be removed and replaced when its energy depletes. When the main battery Low Battery Warning appears (the Status LED remains a steady red) perform an orderly shut down, minimizing the operation of any installed devices and insuring any information is saved that should be saved.

Note: Once you receive the main battery Low Battery Warning, you have approximately 5 minutes to perform an orderly shutdown and replace the main battery pack before the device powers off. The Low Battery Warning will transition the mobile device to Suspend before the device powers off.

Backup Battery

The HX2 has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 50 mAh Nickel Cadmium (NiCd) battery that is factory installed in the unit. The energy needed to maintain the backup battery near full charge at all times comes from the HX2 main battery.

It takes several hours of operation before the backup battery is capable of supporting the operation of the mobile device. The duration of backup battery life is dependent upon operation of the HX2, its features and any operating applications.

The backup battery has a minimum service life of two years. The backup battery is replaced by LXE.

The backup battery can be discharged, recharged and conditioned using a CE Control Panel applet. Tap **Start | Settings | Control Panel | Battery** then tap the Discharge button.

Handling Batteries Safely

- Never dispose of a battery in a fire. This may cause an explosion.
- Do not replace individual cells in a battery pack.
- Do not attempt to pry open the battery pack shell.
- Be careful when handling any battery. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it using proper procedures.

Caution 	Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.
Caution 	NiCd and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

Software

Operating System and Software Load

There are several different aspects to the setup, configuration and operation of the HX2. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this section are to be used as examples only, the configuration of your specific HX2 computer may vary. The following sections provide a general reference for the configuration of the HX2 and some of its optional features.

Operating System

Your HX2 operating system is Microsoft® Windows® CE 5. The HX2 operating system revision is displayed on the Desktop. This is the LXE factory default setting for the Desktop Display Background.

Windows CE Operating System

Note: For general use instruction, please refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the HX2

This segment assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the HX2 and its Windows CE environment.

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with the HX2 keyboard. These are standard keyboard shortcuts for Windows CE applications.

Press these keys …	To …
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + Z	Undo
DELETE	Delete
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
ALT+ESC	Cycle through items in the order they were opened.
CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
ESC	Cancel the current task.

The touchscreen provides equivalent functionality to a mouse:

- A touch on the touchscreen is equivalent to a left mouse click.
- Many items can be moved by the “drag and drop” method, touching the desired item, moving the stylus across the screen and releasing the stylus in the desired location.
- A double stylus tap is equivalent to a double click.
- A touch and hold is equivalent to a right mouse click[1].

[1]Some applications may not support this right click method. Please review documentation for the application to see if it provides for right mouse click configuration.

Warmboot

A warmboot reboots the computer without erasing any registry data. However, any applications installed to RAM are lost, as is all data in RAM. This occurs because the operating system is stored on the flash drive, but must be loaded into RAM to run.

All registry configurations are automatically preserved. Any applications stored as .CAB files in the System folder and configured in the Registry to persist are reinstalled on boot up by the Launch utility.

Coldboot

A coldboot reboots the computer, erases all registry data and returns the computer to factory default settings. In order to be preserved, applications and data must be stored in the System folder. Registry information is not preserved. Only factory default applications and drivers stored as .CAB files in the System folder are loaded by Launch.

A cold boot is initiated by running the Coldboot application in the Windows folder. This application automatically cold boots the HX2, erasing any customer applied registry changes and returning the HX2 to its factory settings.

Clearing Persistent Storage / Reset to Default Settings

The coldboot utility sets all registry settings back to LXE factory defaults. No other clearing is available or necessary.

Folders Copied at Startup

The following folders are copied on startup:

System\Desktop	copied to	Windows\Desktop
System\Favorites	copied to	Windows\Favorites
System\Fonts	copied to	Windows\Fonts
System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs
AppMgr	copied to	Windows\AppMgr
Recent	copied to	Windows\Recent

This function copies only the folder contents, no sub-folders.

The Windows\Startup folder is not copied on startup because copying this folder has no effect on the system or an incorrect effect.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by Launch.

Saving Changes to the Registry

The HX2 saves the registry when you:

- Tap Start | Run then type Warmboot. Tap OK.
- Perform a Suspend / Resume function (by pressing the Pwr key and then pressing it again).

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g. 0 seconds)

The registry is automatically saved every 20 minutes. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g. Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

When you tap Start | Run then type Coldboot and tap the OK button, factory default registry settings are loaded during coldboot. All customized changes and settings are lost.

Software Load

The software loaded on the HX2 consists of Microsoft® Windows® CE 5 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Full Operating System License: Includes all operating system components, including Microsoft® Windows® CE 5 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touchscreen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth (Optional)

Note: Please contact your LXE representative for software updates and CAB files as they are released by LXE.

Software Applications

The following applications are included:

- WordPad
- LXE Scan Wedge (barcode result manipulation)
- ActiveSync
- Transcriber
- Internet Explorer

Bluetooth (Optional)

Start | Settings | Control Panel | Bluetooth

Only installed on a Bluetooth equipped HX2. The System Administrator can Discover and Pair targeted Bluetooth devices for each HX2. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly name for each HX2.

The Bluetooth control panel can also be accessed by doubletapping the Bluetooth icon in the taskbar or on the desktop.

Java (Optional)

Installed by LXE. Files can be accessed by tapping **Start | Programs | JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of Java examples and Plug-ins is also installed with the Java option. LXE does not support Java applications running on the mobile device.

LXE RFTerm (Optional)

Start | Programs | RFTerm

Installed by LXE. The application can also be accessed by double clicking the RFTerm desktop icon.

Avalanche

The Wavelink Avalanche Enabler installation file is loaded on the HX2 by LXE; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. Following installation, the Wavelink Avalanche Enabler will be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

Software Development

See Also: LXE CE API Programming Guide

The LXE CE API Programming Guide documents LXE-specific API calls for the HX2. It is intended as an addition to Microsoft Windows CE API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found on LXE's Developer Portal. For more information and to access the portal, go to www.lxe.com/developer or contact your LXE representative.

Access Files on the Flash Card

Click the **My Device** icon on the Desktop then click the **System** icon.

A flash card is used for permanent storage of the HX2 drivers, CAB files and utilities. It is also used for registry content back up.

CAB files, when executed, are not deleted.

Note: Always perform a warm reset (Start / Run / Warmboot) when exchanging one flash card for another.

HX2 Utilities

The following files are pre-loaded by LXE.

LAUNCH.EXE

Launch works in coordination with registry settings to allow drivers or applications to be loaded automatically into DRAM at system startup. Registry settings control what gets launched; see the App Note for information on these settings. For examples, you can look at the registry key

HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist

Launch will execute .CAB files, .BAT files, or .EXE files.

App Note

All applications to be installed into persistent memory must be in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and are copied to the CE device using ActiveSync, or using a Compact Flash ATA card. The CAB files are copied from ATA or using ActiveSync Explore into the folder System, which is the persistent storage virtual drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist, as follows. The main subkey is any text, and is a description of the file. Then 3 mandatory values are added:

FileName is the name of the CAB file, with the path (usually \System).

Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file.

FileCheck is the name of a file to look for to determine if the CAB file is installed. This will be the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

There are three optional fields that may be added:

1. Order is used to force a sequence of events. Order=0 is first, and Order=99 is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.
2. Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.
3. PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

- The launch utility opens the registry database and reads the list of CAB files to auto-launch.
- First it looks for FileName to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the Installed flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it.
- If the Installed flag is set, auto-launch looks for the FileCheck file. If it is present, the CAB file is installed, and that registry entry is complete. If the FileCheck file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
- Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.

- To force execution every time (for example, for AUTOEXEC.BAT), use a FileCheck of “dummy”, which will never be found, forcing the item to execute.
- For persist keys specifying .EXE or .BAT files, the executing process is started, and then Launch will continue, leaving the loading process to run independently. For other persist keys (including .CAB files), Launch will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.
- Note that the auto-launch process can also launch batch files (*.BAT), executable files (*.EXE), registry setting files (*.REG), or sound files (*.WAV). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Note: Registry entries may vary depending on software revision level and options ordered with the HX2.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the System folder, Launch automatically copies all of the files in these directories to the respective folder on the flash drive:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help
- Programs
- Recent

Note: Files in the Startup folder are executed, but only from System | Startup. They are not copied to another folder.

REGEDIT.EXE

Registry Editor – LXE recommends caution when editing the Registry and also recommends making a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

REGDUMP.EXE

Registry dump – Saves a copy of the registry as a text file. The file, REG.TXT, is located in the root folder.

Note: The REG.TXT file is not saved in persistent storage. To use the REG.TXT file as a reference in the event of a coldboot, LXE recommends copying the file to the System folder on the HX2 or storing a copy of the REG.TXT file on a PC.

WARMBOOT.EXE

Double click this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

Command-line Utilities

Command line utilities can be executed by Start | Run | [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all RAM is erased).

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap Start | Run and type **prtscrn** and tap OK, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and the screen captured file (*scrnnnnn*.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

Desktop

For general use instruction, please refer to commercially available Windows CE user's guides or the Windows on-line Help application installed in the mobile device.

The HX2 Desktop appearance is similar to that of a desktop PC running Windows 2000 or XP.

At the bottom of the screen is the Start button. Tapping the Start Button causes the Start Menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

Desktop Icons

At a minimum, the desktop displays icons for My Device, Internet Explorer and the Recycle Bin. Following are a few of the other icons that may be on the HX2 Desktop. Contact your LXE representative about the latest updates and upgrades for your operating system.

Icon	Function
 My Device	Access files and programs.
 Recycle Bin	Storage for files that are to be deleted.
 Bluetooth	Discover and then pair with nearby discoverable Bluetooth devices.
 My Documents	Storage for downloaded files / applications.
 Internet Explorer	Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from LXE).
 Summit Client Utility	Used for accessing the appropriate wireless configuration, SCU (Summit Client Utility).
 eXpress Scan	The eXpress Scan utility allows an administrator to scan barcodes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the LXE device. eXpress Scan uses barcodes created with eXpress Config.
 LXE RFTerm	RFTerm is an optional terminal emulation program for LXE devices with a Windows operating System. When RFTerm is installed, this icon is displayed on the desktop.

Icon	Function
 Remote Desktop Connection	A shortcut to the Remote Desktop Configuration utility.
 Avalanche	Wavelink® Avalanche Mobility Center™ (Avalanche MC) is a remote client management system that is designed to distribute software and configuration updates to monitored devices, including LXE® computers with Microsoft® Windows® CE. The enabler for Wavelink Avalanche is loaded on the LXE device but not installed. When the enabler is installed this icon is displayed on the desktop.
 Java	Installed by LXE. Tapping the desktop icon displays information on the Java version installed. Files can be accessed by tapping **Start | Programs | JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of Java examples and Plug-ins is also installed with the Java option. LXE does not support Java applications running on the mobile device.
	Start button. Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

Taskbar

The number and type of icons displayed are based on the device type, installed options and configuration of the HX2.

My Device Folders

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System	Internal SD Flash Card (CAB file storage)	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

Wavelink Avalanche Enabler (Optional)

Note: If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device(s).

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager.

After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

- IP address: DHCP or static IP
- RF network SSID
- DNS hosts (primary, secondary, tertiary)
- Subnet mask
- Enabler update

Related Manual: *Using Wavelink Avalanche on LXE Windows Computers*

The HX2 has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped from LXE. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the *Avalanche Update Settings* panel through the *Enabler Interface*.

The designation of the mobile device to the Avalanche CE Manager is LXE_HX2.

LXE CE devices manufactured before October 2006 must have their drivers and system files upgraded before they can use the Avalanche Enabler functions. Contact your LXE representative for details on upgrading the mobile device baseline.

Internet Explorer

Start | Programs | Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the “?” button to access Internet Explorer Help.

Start Menu Program Options

The following list represents the factory default program installation. Your system may contain different items from those shown below, based on the software and hardware options purchased.

Communication	Stores Network communication options
ActiveSync	Transfer files between a HX2 and a desktop computer
Connect	Run this command after setting up a connection
Start FTP Server	Begin connection to FTP server
Stop FTP Server	End connection to FTP server
Command Prompt	The command line interface in a separate window
eXpress Scan	Option. Requires Wavelink Avalanche option eXpress Config.
Internet Explorer	Access web pages on the world wide Internet
Java	Optional
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server
RFTerm	Option. Terminal emulation application.
Settings	Access to all Control Panels, a shortcut to the Network and Dialup Control Panel and access to Taskbar options.
Summit	Set Summit radio / network parameters
Transcriber	Enter data using the stylus on the touchscreen
Wavelink Avalanche	Option. Remote management for networked devices
Windows Explorer	File management program

- If installed, RFTerm runs automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.
- If installed and pre-configured, Wavelink Avalanche connects remotely and downloads updates automatically during each reboot.

Communication

Start | Programs | Communication

ActiveSync

ActiveSync is pre-loaded on all LXE mobile devices.

Using Microsoft ActiveSync you can copy files from your HX2 to your desktop computer , and vice versa.

Once an ActiveSync relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the HX2.

Connect and LXEConnect

Upon cabling your HX2 to the desktop/laptop, and ActiveSync on the desktop/laptop opens, if the Connect or LXEConnect installation does not open on your HX2, Contact your LXE representative for assistance.

Start FTP Server / Stop FTP Server

Start | Communication | Start (or Stop) FTP Server

These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

Summit

Start | Settings | Control Panel | Summit

Use this option to set up radio client profiles.

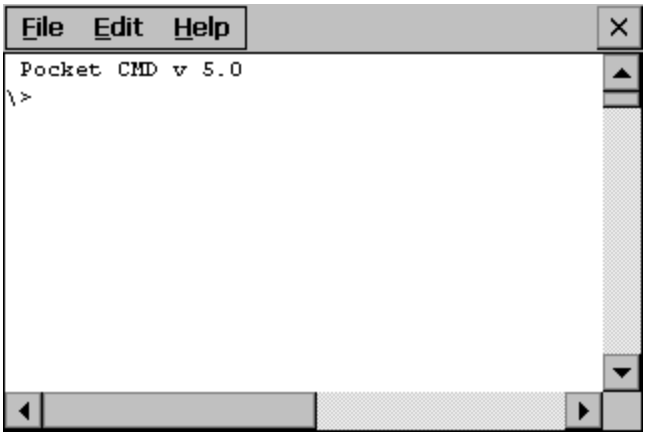
The Summit Control Panel can also be accessed by doubletapping the Summit icon in the taskbar or on the desktop.

Certs

The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication.

Command Prompt

Start | Programs | Command Prompt



Pocket CMD Prompt Screen

Type **help cmd** at the command prompt to view valid Pocket PC (Console) commands.

Exit the command prompt by typing **exit** at the command prompt or tap **File | Close.**

eXpress Scan

The eXpress Scan utility allows an administrator to scan barcodes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the HX2.

eXpress Scan uses barcodes created with eXpress Config.

Internet Explorer

Start | Programs | Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the ? button to access Internet Explorer Help.

Microsoft Wordpad

Start | Programs | Microsoft WordPad

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad.

By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g. .RTF or .DOC.

Tap the ? button to access WordPad Help.

Remote Desktop Connection

Start | Programs | Remote Desktop Connection

There are few changes in the Windows CE version of Remote Desktop Connection as it relates to the general desktop Windows PC Microsoft Remote Desktop Connection options.

If installed, Remote Desktop Connection on the HX2 can be accessed by **Start | Programs | Remote Desktop Connection**.

Select a computer from the drop down list or enter a host name and tap the Connect button.

Tap the Options >> button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the ? button to access Remote Desktop Connection Help.

Settings

Start | Settings

The Settings menu option may include the following:

Control Panel	All control panels
Network	Shortcut to the *Network and Dialup Connections* control panel. Connect to a network, create a new connection, and adjust parameters for client connections.
Taskbar	Set Taskbar parameters

Transcriber

To make changes to the Transcriber application, tap the keyboard icon in the status bar. Select Transcriber from the pop-up menu. Then open the Input control panel and tap the Options button. Transcriber Options (Start | Settings | Control Panel | Input Panel) are available only when Transcriber is selected as the active input method. Tap the “?” button or the Help button to access Transcriber Help.

Windows Explorer

Start | Programs | Windows Explorer

There are a few changes in the Windows CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the “?” button to access Windows Explorer Help.

Taskbar

Start | Settings | Taskbar and Start Menu

There are a few changes in the Windows CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options.

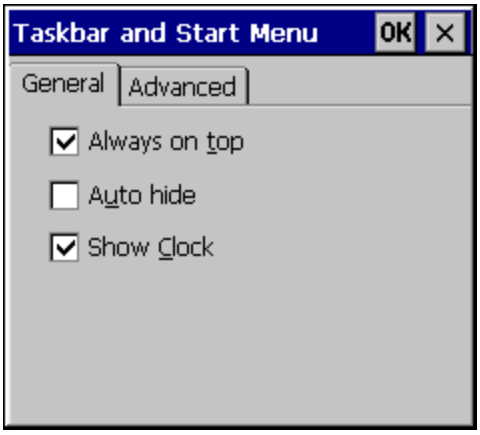
When the taskbar is auto hidden, press the Ctrl key then the Esc key to make the Start button appear.

Clicking the Taskbar option on the Settings menu displays theTaskbar General tab and the Taskbar Advanced tab.

General Tab

Factory Default Settings

Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled



Taskbar Properties, General Tab

Advanced Tab

Taskbar Properties, Advanced Tab

Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the Settings | Control Panel menu option.

Clear Contents of Document Folder

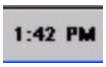
Tap the Clear button to remove the contents of the Document folder.

Taskbar Icons

As HX2 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to **Start | Help** for an explanation of standard Windows CE taskbar icons.

Following are a few of the HX2 and LXE unique taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

Icon	Function
	Wireless Zero Config Inactive / Connected / Not Connected. Clicking on the icon opens the Wireless Zero Config utility.
	Bluetooth connected / disconnected. Clicking the icon opens the Bluetooth control panel.
	ActiveSync Connection
	Cerdisp connected (displayed when LXEConnect is connected)
	Summit Client signal indicator no signal/ excellent signal. Clicking on the icon opens the Summit Client Utility.
	Battery charge indicator. Percent of battery charge is indicated.
	External power connected
	Current time. Clicking the time display opens the Date/Time control panel.
	Click this icon to return to the Desktop.
	AppLock switchpad.
	Input method, keyboard / input panel / transcriber
	CapsLock active
	No modifier key is in focus
	Green modifier key active
	Orange modifier key active
	Blue modifier key active

Icon	Function
	Shift modifier key active
	Multiple modifier keys active, Green plus Orange / Shift plus Blue

HX2 OS Upgrade

Introduction

Depending on the size of the operating system, the total time required for a successful upgrade may require several minutes.

The OS upgrade files are unique to your HX2 physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

Preparation

- Please Contact your LXE representative to get the **OS upgrade files** from LXE.
- Use ActiveSync to back up HX2 user files and store them elsewhere before beginning an upgrade on the HX2.
- Maintain an uninterrupted AC/DC power source to the HX2 throughout this process.
- The SD / CF card with the OS and systems files must be present for the HX2 to boot. LXE recommends that removal or installation of SD or CF cards be performed on a clean, well-lit surface.
- Always perform OS updates when the HX2 has a dependable external power source connected to the HX2 and/or a fully charged main battery.

Procedure

1. Verify a dependable power source is applied to the HX2 and will stay connected during the upgrade procedure.
2. Establish an ActiveSync connection between the HX2 and a desktop/laptop computer.
3. Download the OS files from the desktop/laptop to the HX2's System folder.
4. During the file copy process to the HX2 System folder, when asked “Overwrite ?”, select Yes to All.
5. Review the files that were downloaded to the System folder.
6. Restart the HX2.
7. Disconnect from ActiveSync.
8. When the OS finishes loading, check the OS update version by selecting **Start | Settings | Control Panel | About | Software** tab.

The touch screen may require calibration, however most Windows OS versions save the calibration data, eliminating the need to calibrate.

Battery State and OS Upgrade

LXE recommends a fully charged main battery be cabled to the HX2 prior to reflashing or upgrading the operating system. A prompt may appear when the battery reaches Critical Low that informs the user there is not enough power in the main battery to perform the upgrade.

The operating system will not be able to execute the OS update when the battery level is too low (25% or less), as there is a high risk that the power remaining in the battery expires when executing the upgrade and the HX2 will be left in an inoperable state.

When main battery power level is too low, connect external power to the HX2 before performing the upgrade procedure. Do not disconnect external power before the upgrade process is complete.

Troubleshooting

The powered device won't boot up after the upgrade is finished.

Send the HX2 to LXE Service and Support for re-imaging.

Warning: Opening the device e.g. removing endcaps or access panels, etc. could void the user's authority to operate this equipment.

Using ActiveSync

Introduction

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the HX2.

Note: ActiveSync serial connection requires a powered HX2 desktop cradle.

Requirement : ActiveSync (version 4.5 or higher for **Windows 2000/XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the PC is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

Using Microsoft ActiveSync, you can synchronize information on your desktop computer with the HX2 and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your device to your desktop computer,
- set up a partnership so you can synchronize information between your device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The initial setup of ActiveSync must be made via a USB or serial connection. When there is a Connect icon on the desktop, this section can be bypassed.

Partnerships can only be created using USB cable connection. After the partnerships are established, ActiveSync communication can be initiated using USB or wireless, or, using a cradle, serial.

Connect via USB

The default connection type is **USB Client**

To change the connection type or to verify it is set to USB, select **Start | Settings | Control Panel | PC Connection**.

Tap the Change button. From the popup list, choose

USB Client

This will set up the mobile device to use the USB port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

IMPORTANT – DO NOT PUT THE MOBILE DEVICE INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Connect the correct cable to the PC (the host) and the mobile device (the client) as detailed below. USB will start automatically when the USB cable is connected, not requiring you to select "Connect" from the start menu.

Cable for USB ActiveSync Connection:

If a cradle is used:

HX2312DSKCRDL or HX2313DSKCRDL - HX2 desk cradle

Use with **standard USB cable** with type A plug for PC/Laptop USB port and type B plug for HX2 cradle USB type B client port.

- Plug the type B end of the standard USB cable plug into the USB type B port on the HX2 cradle (port #2).
- The USB type A connector on the standard cable connects to a USB port on a PC or laptop.
- The USB client (port #1) connector on the cradle does not need to be connected.

If a cradle is not used:

HX2001CABLE - ActiveSync cable for HX2 when not in the desk dock. Cable connects directly to the HX2 and the other end connects to PC/Laptop USB port.

- Insert the HX2 cable end into the cradle connector on the bottom of the HX2.
- The USB type A connector on the cable connects to a USB port on a PC or laptop.

Note: The ActiveSync cable for the HX2 does not appear to fit tightly with the cradle connector, as shown above. This is normal.

Serial Connection

To change the connection type select **Start | Settings | Control Panel | PC Connection.**

Tap the Change button. From the popup list, choose

Serial 1 @ 57600

This will set up the mobile device to use the serial port on the cradle. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

Select Start | Settings | Scanner and ensure the scanner is set to a port that is NOT the same as the ActiveSync port.

Connect the correct cable to the PC (the host) and the mobile device (the client) cradle. Select "Connect" from the Start Menu on the client (Start | Programs | Communications | Connect).

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Wireless Connection

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the mobile device. The initial partnership must be done using USB cable connection.

Once the relationship is established, the ActiveSync link in the Start Menu gives a choice of connections, one of which is Network.

Select **Start | Settings | Programs | Communication | ActiveSync**. From the popup list, choose Network and then tap the Connect button.

Synchronizing from the Mobile Device

To synchronize using a wireless LAN card, you must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

To initiate synchronization from your device, tap **Start | Programs | Communication | ActiveSync** to begin the process.

Tap **Sync** to connect and synchronize. View synchronization status.

Tap **Tools** to synchronize or change synchronization settings. View connection status.

Tap **Stop** to stop synchronization.

Tap **Start | Help** for context-sensitive help.

Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows image. This, however, includes most of the files in the \Windows folder).

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

A partnership between the mobile device and ActiveSync has been established.

Serial Port Transfer

- A desktop or laptop PC with an available serial port and a mobile device with a serial port. The desktop or laptop PC must be running Windows NT or greater.
- Null modem cable with all control lines connected.

USB Transfer

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows 98 SR2 or greater.
- Use the LXE-specific USB cable as listed in Connect Via USB.

Connect

Connect the modem cable to the PC (the host) and the mobile device (the client). Select “Connect” from the Start Menu on the mobile device (Start | Programs | Communications | Connect).

Note: Run “Connect” when the “Get Connected” wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB synchronization will start automatically when the cable is connected, not requiring you to select “Connect” from the Start menu.

Disconnect

USB Connection

- Disconnect the cable from the mobile device or cradle.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IMPORTANT – Do not put the mobile device into Suspend while connected via USB. The device will be unable to connect to the host PC when it resumes operation.

Serial Connection

- Disconnect the cable from the cradle.
- Put the mobile device into Suspend.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Network Connection

- Put the mobile device into Suspend.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (Control Panel | System | Device Name)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy that partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

Troubleshooting ActiveSync

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the HX2 is connected to a PC by a cable, disconnect the cable from the HX2 and reconnect it again.

Check that the correct connection is selected (Serial or USB “Client” if this is the initial ActiveSync installation).

See Also: “Cold Boot and Loss of Host Reconnection”.

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host turns green and spins, but connection never occurs

Baud rate of connection is not supported or detected by host. Check that the correct connection is selected (Serial or USB “Client” if this is the initial ActiveSync installation).

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

Solution 1: ActiveSync icon on the PC does not turn green after connecting USB cable from HX2.

1. Disconnect HX2 USB cable from PC.
2. Suspend/Resume or Restart the HX2.
3. In ActiveSync | File | Connection Settings on PC disable Allow USB Connections and click OK.
4. Re-enable Allow USB Connections on the PC and click OK.
5. Reconnect USB cable from HX2 to PC.

Solution 2: The host doesn’t know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Testing connection with a terminal emulator program, or a serial port monitor

You can use HyperTerminal or some other terminal emulator program to do a rough test of ActiveSync. Set the terminal emulator to 8 bits, no parity, 1 stop bits, and the same baud rate as the connection on the CE device. After double-tapping REPLLOG.EXE on the CE device, the word “CLIENT” appears on the display in ASCII format. When using a serial port monitor, you see the host echo “CLIENT”, followed by “SERVER”. After this point, the data stream becomes straight (binary) PPP.

Configuring the HX2 with LXEConnect

LXEConnect allows a user to view the HX2 screen remotely from a PC using an ActiveSync connection:

Requirement : ActiveSync (version 4.5 or higher for **Windows 2000/XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the PC are available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

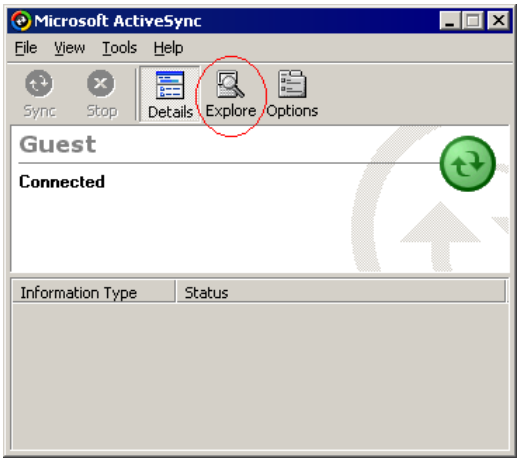
Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

ActiveSync is already installed on the HX2. The HX2 is preconfigured to establish a USB ActiveSync connection to a PC when the proper cable is attached to the HX2 and the PC.

If the HX2 uses a serial port for ActiveSync, it will be necessary to configure the HX2 to use the serial port. Complete details on the proper cables and port configuration are included in Initial Setup.

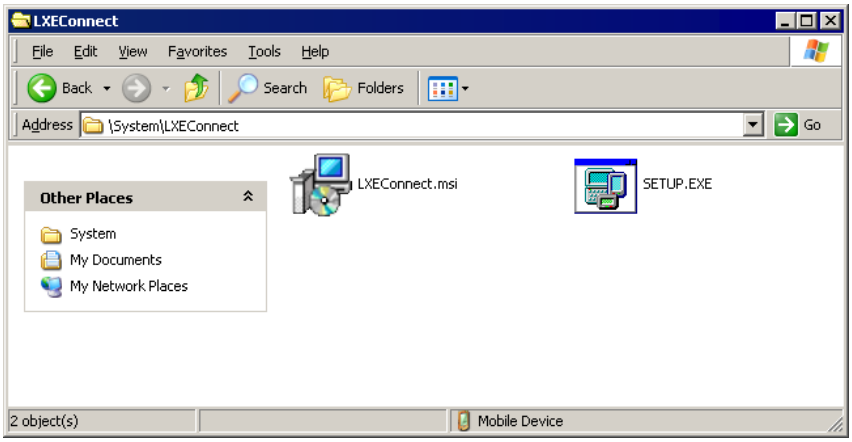
Install LXEConnect

1. Install Microsoft ActiveSync on a PC with a USB port. For details, please see Initial Setup.
2. Power up the HX2.
3. Connect the HX2 to the PC using the proper connection cable. Once connected, the ActiveSync dialog box appears. If using the USB connection, the ActiveSync connection is automatically established. If using a serial connection, it is necessary to initiate the connection from the HX2.
4. Select “No” for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use LXEConnect. However, if a partnership is desired for other reasons, one may be established now. More details on partnerships are included in ActiveSync Help.
5. When the ActiveSync screen appears, select Explore.



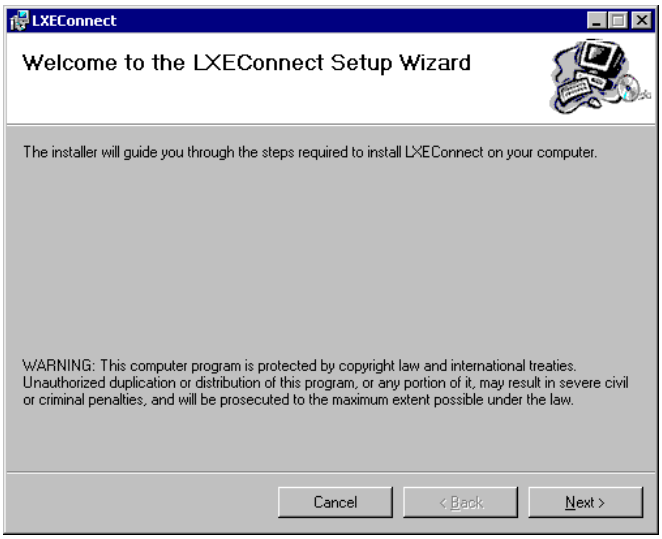
ActiveSync Explore

6. An explorer window is displayed for the HX2. Browse to the \System\LXEConnect folder. If this folder is not present, contact your LXE representative for the necessary files.



LXEConnect Installation Files

7. Select and copy the LXEConnect.msi and Setup.exe files from the HX2 to the user PC. Note the location chosen for the files.
8. Close the ActiveSync explorer dialog box. Do not disconnect the HX2 ActiveSync connection.
9. Execute the setup.exe file that was copied to the user PC. This setup program installs the LXEConnect utility.

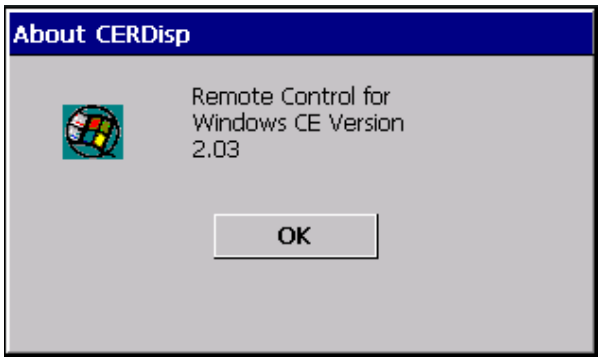


LXEConnect Setup

10. Follow the on screen installation prompts. The default installation directory is C:\Program Files\LXE\LXEConnect.
11. When the installation is complete, create a desktop shortcut to the following file: C:\Program Files\LXE\L-XEConnect\LXEConnect.exe. If a different directory was selected during installation, please substitute the appropriate directory.
12. LXEConnect is now installed and ready to use.

Using LXEConnect

1. If an ActiveSync connection has not been established, connect the HX2 to the PC.
2. Double-click the LXEConnect icon that was created on the PC desktop.
3. LXEConnect launches.



LXEConnect Notice

4. Click the OK button to dismiss the About CERDisp dialog box on the desktop by clicking the OK button in the LXE-Connect window on the PC desktop.. The dialog box automatically times out and disappears after approximately 30 seconds.

LXEConnect Desktop

5. The HX2 can now be configured from the LXEConnect window. Input from the PC's mouse and keyboard are recognized as if they were attached to the HX2.
6. When the remote session is completed, terminate the LXEConnect program by selecting File | Exit or clicking on the X in the upper right hand corner to close the application, then disconnect the ActiveSync cable.

Note: After using LXEConnect, the HX2 cannot go into Suspend mode until after a warmboot. If using Power Management on a HX2, always warmboot the HX2 when finished using LXEConnect.

Control Panel

Start | Settings | Control Panel or My Device | Control Panel link

Note: Change the font displayed on the touchscreen by choosing Start | Settings | Control Panel | Keyboard and then the Key map dropdown list.

Tap the ? button for Help when changing HX2 Control Panel options.

Option	Function
About	Software, hardware, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	LXE AppLock Administration utility.
Battery	View voltage and status of the main and backup batteries.
Bluetooth	Set the parameters for Bluetooth device connections.
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Device Management	Allows a Device Management client (the device equipped with a Microsoft Windows CE operating system) to work with a Microsoft Systems Management Server.
Dialing	Connection setup for modem attached to COM port or Compact Flash slot.
Display	Set background graphic and scheme. Set touchscreen and keypad backlight properties and timers.
HX2-3 Options	Set various device specific configuration options.
Input Panel	Select the current key / data input method. Select custom key maps.
Installed Programs	View the list of installed programs. In some OS versions this panel replaced Remove Programs. Contact your LXE representative.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
Keypad	Configure Alpha key, KeyMap keys, RunCmd and LaunchApp.
License Viewer	Displays license information for installed licensed applications.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Network Capture	Set network logging options.
Owner	Set the mobile device owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password	Set OS access password properties for signon and/or screen saver.

Option	Function
PC Connection	Control the connection between the mobile device and a local desktop or laptop computer.
Power	Set Power scheme properties. Review device status and properties.
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	Select to remove specific **user installed** programs in their entirety. In some OS versions this panel has been replaced by Installed Programs.
Scanner	LXE Scan Wedge utility. Set scanner key wedge, scanner port, and imager LED illumination options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign scanned barcode data manipulation parameters.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound WAV files to events.
WiFi	Set the parameters for a Summit client.

About

Start | Settings | Control Panel | About

The data cannot be edited by the HX2 user on these panels.

Tab	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	Revision level of LXE software modules and .NET Compact Framework Version.
Network IP	Current network connection IP and MAC address. Only the first 2 network ports are shown (usually radio and ActiveSync).

Version window information is retrieved from the registry.

Version Tab and the Registry

Modify the Registry using the Registry Editor. LXE recommends caution when editing the Registry and also recommends making a backup copy of the registry before changes are made.

The registry settings for the Version tab are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window .

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Language and Fonts

The Software tab displays any fonts built into the OS image. The fonts built into the OS image are noted in the Language section of this tab:

- English only – No additional fonts are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian fonts are ordered separately and built-in to the OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the (English only) default (extended) fonts.

When an Asian font is copied into the fonts folder on the /System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in Regional Settings control panel, the font does not work for naming desktop icons with Asian names, the font does not work for third-party CE applications, the font does not work for some third-party MFC applications.

Identifying Software Versions

The Versions tab displays the versions of many of the software programs installed. Not all installed software installed on the mobile device is included in this list and the list varies depending on the applications loaded on the HX2. The LXE Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

MAC Address

The Network IP tab displays the MAC address of the network card.

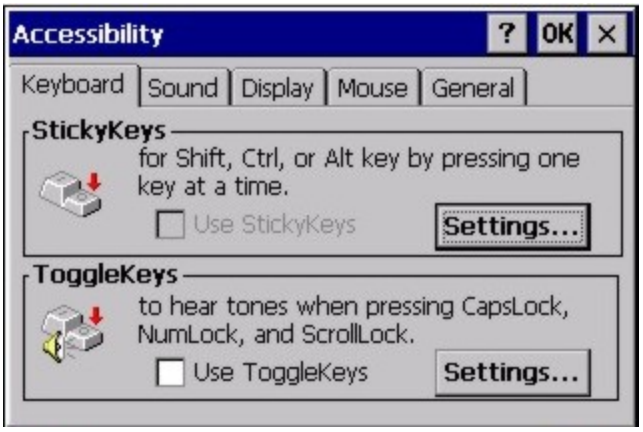
Accessibility

Start | Settings | Control Panel | Accessibility

Customize the way the HX2 keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general Windows desktop Accessibility options.

Note: LXE disables the keypad StickyKeys and StickyKeys Settings on the Keyboard panel as this setting, when enabled, interferes with LXE's assigned sticky key implementation.

Tab	Contents
Keyboard	Sticky Keys - Disabled. ToggleKeys - Disabled by default. Tap the *Use ToggleKeys* checkbox to enable this option. Tap the Settings button to view or change parameters.
Sound	SoundSentry is disabled by default. Tap the *Use SoundSentry* checkbox to enable this option. Tap the Settings button to view or change parameters.
Display	High Contrast is disabled by default. Tap the *Use High Contrast* checkbox to enable this option. Tap the Settings button to view or change parameters.
Mouse	MouseKeys is disabled by default. Tap the *Use MouseKeys* checkbox to enable this option. Tap the Settings button to view or change parameters.
General	Automatic reset is disabled by default. Tap the *Turn off accessibility features* checkbox to enable this option and use the dropdown option to assign a timer. Notification is enabled by default. Sounds are emitted when turning a feature on or off.



The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

- If the ToggleKeys option is selected, please note that the ScrollLock key does not produce a sound as the CapsLock and NumLock keys do.
- If the SoundSentry option is selected, please note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.

Administration - for AppLock

Introduction

LXE's AppLock is designed to be run on LXE certified Windows based devices only. LXE loads the AppLock program as part of the LXE customer installation process.

HX2 AppLock is setup by the Administrator by tapping Start | Settings | Control Panel | Administration.

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

The assumption, in this chapter, is that the first user to power up a new mobile device is the system administrator.

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other HX2 Control Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

AppLock is updated periodically as new options become available. Contact your LXE representative for assistance, downloads and update availability.

Setup a New Device

LXE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the HX2 is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies the applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

1. Connect an external power source to the device and press the Power button.
2. Adjust screen display, audio volume and other parameters if desired. Install accessories.
3. Tap Start | Settings | Control Panel | Administration icon.
4. Assign applications on the Control (single application) or Application (dual application) tab screen.
5. Assign a password on the Security tab screen.
6. Select a view level on the Status tab screen, if desired.
7. Tap OK
8. Press the hotkey sequence to launch AppLock and lock the configured application(s)
9. The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey

Shift+Ctrl+A

Password

none

Application path and name

none

Application command line

none

End User Mode

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- Corrupted registry settings.

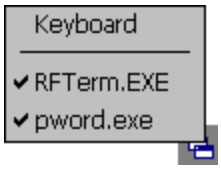
To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Forgotten password?

See: Troubleshooting

End-User Switching Technique

Note: The touch screen must be enabled.



Switchpad Menu

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the HX2 default input method (Input Panel, Transcriber, or custom input method) is activated.

The check to the left of the application name indicates that the application is active.

If the application is listed but does not have a checkmark to the left of the application name, this means the application is configured in AppLock and can be manually launched by clicking on the application name in the list.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

See Also: Application Panel | Launch | Manual (Launch) and Allow Close

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the Activation key. The Activation key is assigned by the Administrator using the Global Key parameter. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: Start | Settings | Administration | Application Panel | Global Key

Hotkey (Activation hotkey)

If the mobile device uses LXE's Multi AppLock to allow the user to switch between applications, the default Activation key is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. Note that the system administrator may have assigned a different key sequence to use when switching applications.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

When the Internet checkbox is enabled, the Menu and Status check boxes are available.

Enabling the Menu checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Application Configuration

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

Settings | Control Panel | Administration icon

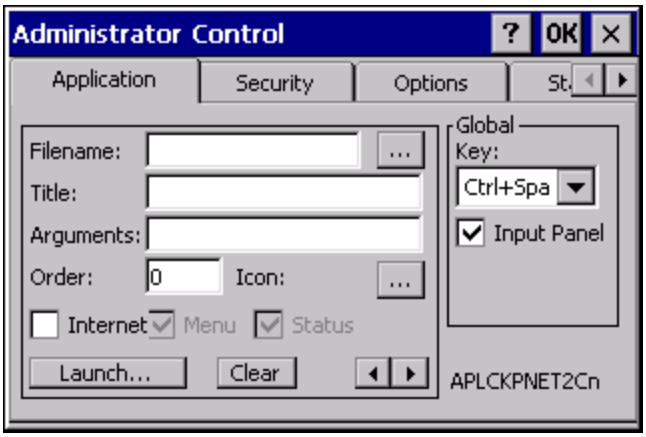
The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Important: Before setting up multiple instances of the same application, make sure the targeted software application will allow two instances to run at the same time.

Application Panel

Note: Users of Single-Application AppLock have a Control tab instead of an Application tab. Some of the options in this section do not apply to the Control tab.



Application Panel

Note: If your Application Panel does not look like the figure shown above, you may have the Single Application version.

Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

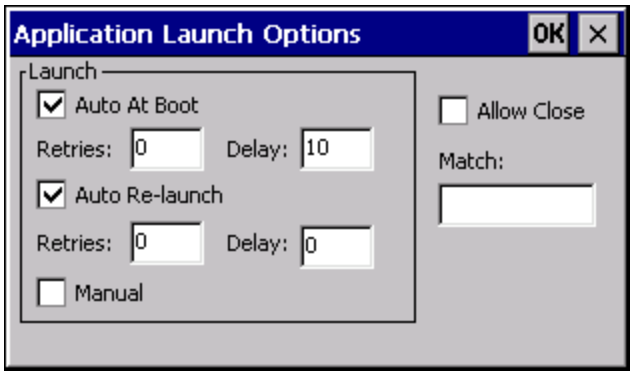
Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order and do not need to be sequential.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.
Launch Button	See following section titled Launch Button. *Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.*
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the Activation key.

Option	Explanation
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. *Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.*
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

Note: The Launch button may not be available in all versions of Multi-AppLock. Contact your LXE representative for assistance, downloads and AppLock update availability.

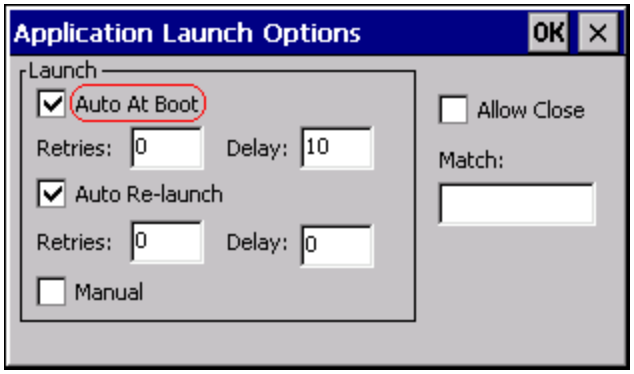
When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



Application Launch Options

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot



Auto At Boot Settings

Default is Enabled.

Auto At Boot

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

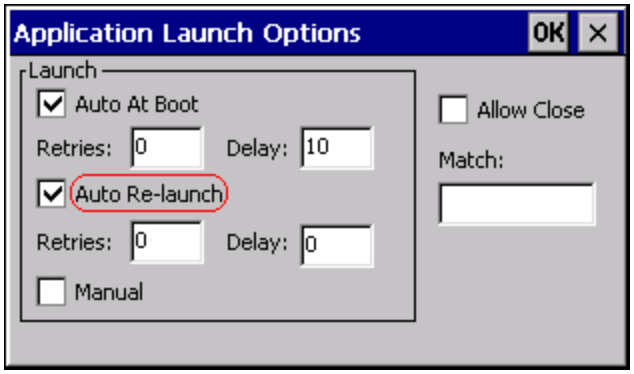
This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch



Auto Re-launch Settings

Auto Re-Launch

Default is Enabled.

When enabled for a specific application. automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Retries

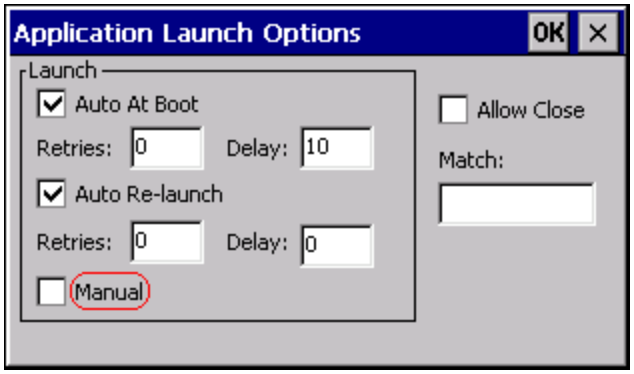
Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)



Manual Launch Checkbox

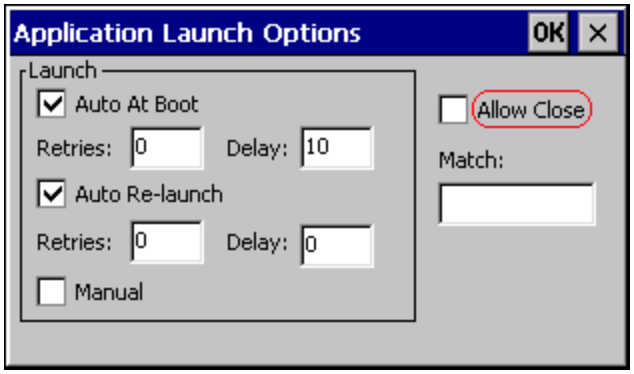
Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Allow Close

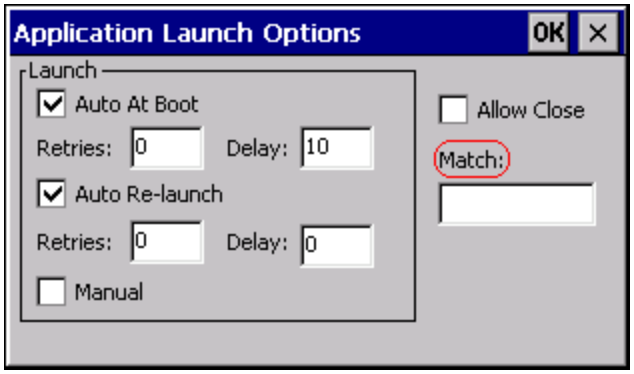


Allow Close Checkbox

Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

Match



Match Textbox

Match

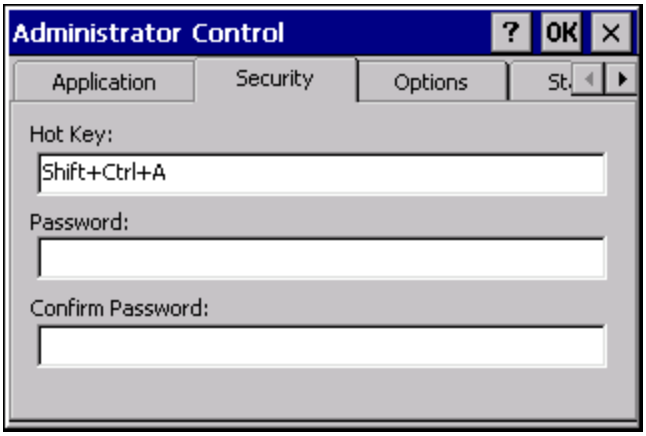
Default is blank (match is not used).

AppLock works by associating display windows with the launched process ID. If an application uses different process IDs for windows it creates, the Match field must be used.

Use the Match field to specify up to 32 characters of the class name for the application.

For example, DOS applications using a standard DOS display box should specify **condev_appcls** in the Match textbox.

Security Panel



Security Panel

Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with “Shift”, “Alt”, and “Ctrl” text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the ‘Ctrl’ key is pressed followed by ‘A’, “Ctrl+A” is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

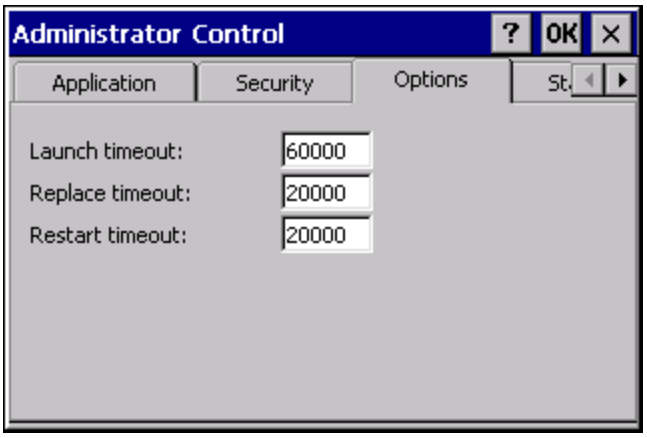
Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: Passwords and Troubleshooting

Options Panel

AppLock contains several types of delays and timeouts to accommodate different applications. Please note that the delays specified on the Launch panel are delays before AppLock attempts to start the specified application(s). The timesouts specified on this panel are delays after AppLock has attempted to launch the application.



Options Panel

Launch timeout

This timeout specifies the period of time for AppLock to wait for the application to initially launch after the application has been called. For example, if the application takes time to launch and then initialize before a display a window is created, use this delay to specify the delay period.

Replace timeout

This timeout specifies the period of time for AppLock to wait after an initial screen (like a password prompt screen) is replaced by another application window.

Restart timeout

This specifies the period of time for AppLock to wait for an application to restart. If the application fails to restart automatically, AppLock then proceeds according to the options selected when the application was configured on the Application and Launch panels.

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.

Status Panel

Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

Note: If your Status Panel does not look like the figure shown above, you may have the Single Application version which does not have as many options.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: Error Messages

Troubleshooting AppLock

The mobile device won't switch from Administration mode to end-user mode.

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word and LXE RFTerm, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. LXE has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

```
Selected hotkey is not allowed. Please reenter.
```

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Can't locate the password that has been set by the administrator?

Contact your LXE representative for assistance.

Battery

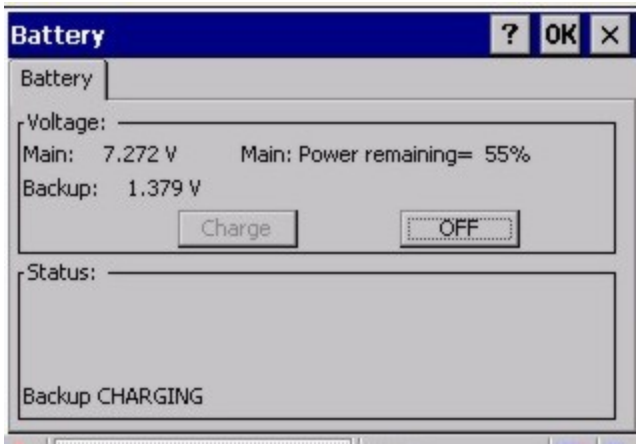
Start | Settings | Control Panel | Battery

This panel is used to view the status and percentage of power remaining in the HX2 main battery. The data cannot be edited by the user.

	The battery gas gauge icon resides in the system tray and shows four levels of charge – 100%, 75%, 50%, 25%. At a point below 25%, the system status LED will turn red and the gas gauge icon will turn red indicating the battery is low.

Jacked is shown in the Status box when the Main battery is receiving external power.

The main battery is charged/recharged when the HX2 is docked in a powered cradle or directly cabled to an external power source.



The backup battery draws power from the Main battery to maintain a charge. The backup battery voltage and percentage of power fluctuate continuously.

When there is no Main battery in the unit, the backup battery begins to discharge as it maintains RAM and other vital settings. After a Main battery is installed, the backup battery begins to draw power from the Main battery again.

Note: Frequent connection to an external power source, if feasible, is recommended to maintain backup battery charge status as the backup battery cannot be recharged by a dead or missing main battery.

Backup Battery Maintenance

LXE recommends Discharging and Recharging the backup battery twice a year. Use the Charge or Discharge buttons to charge and discharge the backup battery:

To Charge

Tap the Charge button. The Discharge button text changes to “Off”. When the backup battery is charging, tap the Off button to stop the Charge process.

To Discharge

Tap the Discharge button. The Charge button text changes to “Off”. When the backup battery is discharging, tap the Off button to stop the Discharge process.

Bluetooth

Start | Settings | Control Panel | Bluetooth

Note: Contact your LXE representative for upgrade availability if your Bluetooth control panel is not the same as the control panels presented in this section.

Discover and manage pairing with nearby Bluetooth devices.

Factory Default Settings

Discovered Devices	None
Settings	
Turn Off Bluetooth	Enabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled
Printer Port on COM 9:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer Friendly Name	System Device Name
Reconnect	
Report lost connection	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled
OPP Setup	
Inbox	\My Device\My Documents\DefaultInbox
Outbox	\My Device\My Documents\DefaultOutbox
Write Capable	Enabled
Enable Notifications	Enabled
Disable LXEZ Pairing OPP	Unchecked, OPP is enabled

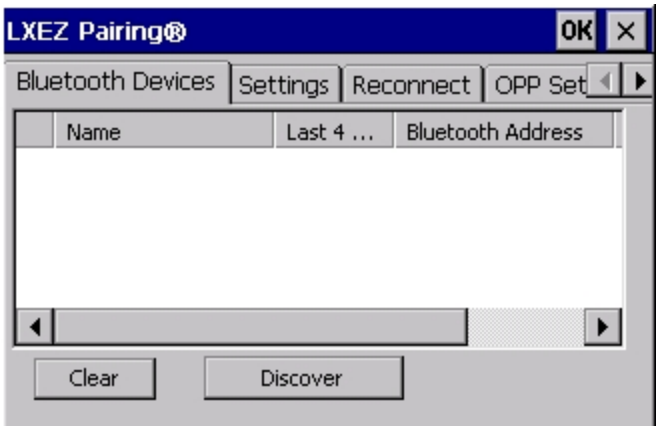
Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the HX2.

- The default Bluetooth setting is On.
- The HX2 cannot be discovered by other Bluetooth devices when the **Computer is discoverable** option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- When **Filtered Mode** is enabled, the HX2 can pair with one Bluetooth scanner and one Bluetooth printer.
- When **Filtered Mode** is disabled, the HX2 can pair with up to four Bluetooth devices, with a limit of one scanner, one printer, two HID[1] devices (one Mouse, one Keyboard), one PAN[2] device, and one DUN[3] device connected at the same time.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the HX2.
- The target Bluetooth device should be as close as possible (up to 32.8 ft (10 meters) Line of Sight) to the HX2 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the HX2. The HX2 operating system has been upgraded to the revision level required for Bluetooth client operation. An application (or API) is available that will accept data from serial Bluetooth devices.

Bluetooth Devices

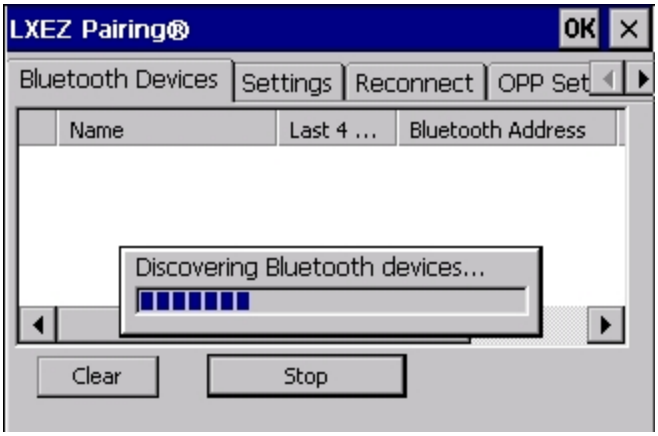
The Bluetooth Devices tab displays any device previously discovered and paired with the HX2.



[1]Human Interface Device profiles used by Bluetooth keyboards, mice, pointing devices and remote monitoring devices.
[2]Personal Area Networking profile. Un-modified Ethernet payloads (using BNEP) can exchange packets between Bluetooth devices. PANU is a PAN User service that uses either the NAP or the GN service.
[3]Dial-Up Networking provides access to the Internet and other dial-up services using Bluetooth technology.

Discover

Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier of each device discovered.

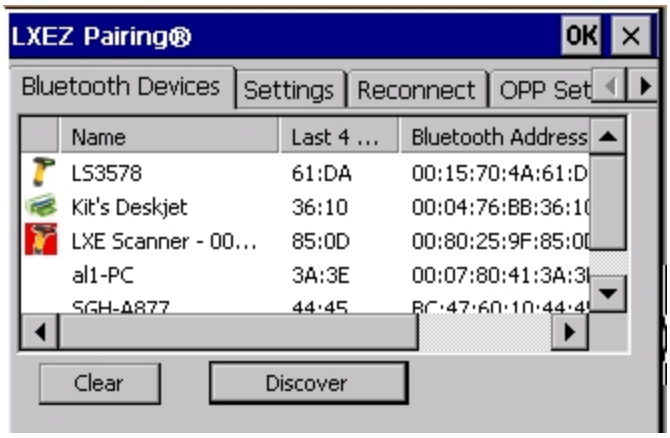


Stop Button

Tap Stop at any time to end the Discover and Query for Unique Identifier functions. Devices not paired are not shown after any reboot sequence.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the HX2 Bluetooth scanning range, the Bluetooth connection between the paired device and the HX2 is lost. There may be audible or visual signals as paired devices disconnect from the HX2.

Bluetooth Device List



The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Scanner or a Printer. The Bluetooth panel assigns an icon to the device name.

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Serial device, a Bluetooth scanner, a Bluetooth printer, a PAN, and a DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard. The Bluetooth panel assigns an icon to the device name.

An icon with a red background indicates the device's Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the HX2 and the device's Bluetooth connection is active.

Double-tap a device in the list to open the device properties menu. The target device does not need to be active.

Clear Button

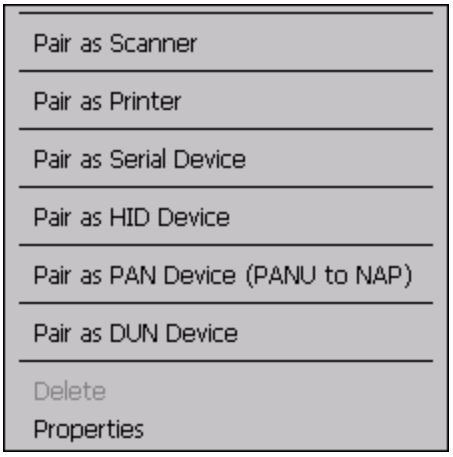
Deletes all devices from the Device table that are not currently paired. A dialog box is presented, "Delete all disconnected devices? Yes/No". Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence. Tap the No button to make no changes. See Clear Pairing Table on Boot.

Bluetooth Device Menu

Pre-requisite: The Discover button has been clicked and there are Bluetooth devices listed.

Click on a device in the list to highlight it. Double click the highlighted device to display the Bluetooth Device right click menu. The Bluetooth device does not need to be active.

Filtered Mode Enabled

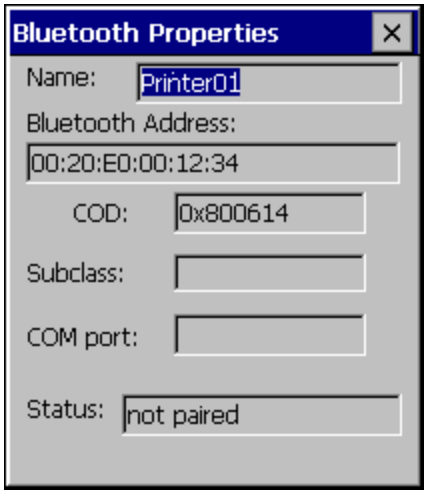


Filtered Mode Disabled

Right Click Menu Options

Pair as Scanner	Receive data from the highlighted Bluetooth scanner or Bluetooth imager.
Pair as Printer	Send data to the highlighted Bluetooth printer.
Pair as Serial Device	Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled.
Pair as HID Device	Communicate with the highlighted HID (Human Interface Device). This option is available when Filtered Mode is disabled/unchecked.
Pair as PAN Device (PANU to NAP)	Communicate with the highlighted PAN (Personal Area Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Pair as DUN Device	Communicate with the highlighted DUN (Dial-Up Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Disconnect	Stop the connection between the HX2 and the highlighted paired Bluetooth device.
Delete	Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the HX2 Bluetooth Devices panel after the user taps OK.
Properties	More information on the highlighted Bluetooth device.

Bluetooth Device Properties



Example - Bluetooth Properties Panel

Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

Settings

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Turn Off Bluetooth

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn Off Bluetooth* to *Turn On Bluetooth*.

Default

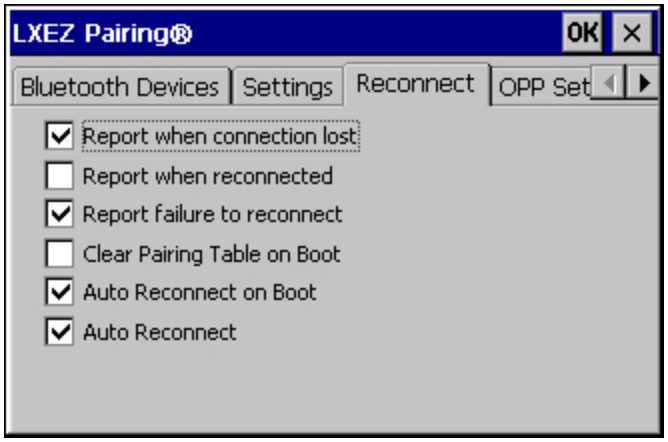
The default value is Bluetooth On.

Options

Option	Function
Computer is connectable	This option is Enabled by default. Disable this option to inhibit HX2 connection initiated by a Bluetooth scanner.
Computer is discoverable	This option is Disabled by default. Enable this option to ensure other devices can discover the HX2.

Option	Function
Prompt if devices request to pair	This option is Enabled by default. A dialog box appears on the HX2 screen notifying the user a Bluetooth device requests to pair with the HX2. The requesting Bluetooth device does not need to have been Discovered by the HX2 before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen. *Note: In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.*
Continuous Search	This option is Disabled by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the HX2 stops searching after 30 minutes. This option draws power from the Main Battery.
Filtered Mode	This option is Enabled by default. Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked). When Filtered Mode is disabled, the HX2 can pair with up to four Bluetooth devices, with a limit of one Bluetooth scanner, one Bluetooth printer, one PAN, and one DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard. A Warmboot is required every time Filtered Mode is toggled on and off.
Printer Port - COM9	This option is Disabled by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be disabled.
Logging	This option is Disabled by default. When logging is enabled, the HX2 creates *bt_log.txt* and stores it in the /System folder. Bluetooth activity logging is added to the text file as activity progresses. A *bt_log_bak.txt* file contains the data stored by *bt_log.txt* prior to reboot. During a reboot process, the HX2 renames *bt_log.txt* to *bt_log_bak.txt*. If a file already exists with that name, the existing file is deleted, the new *bt_log_bak.txt* file is added and a new *bt_log.txt* is created.
Computer Friendly Name	Default: Computer System Name (System Panel | Device Name tab). The name, or identifier, entered in **this** space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

Reconnect



Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

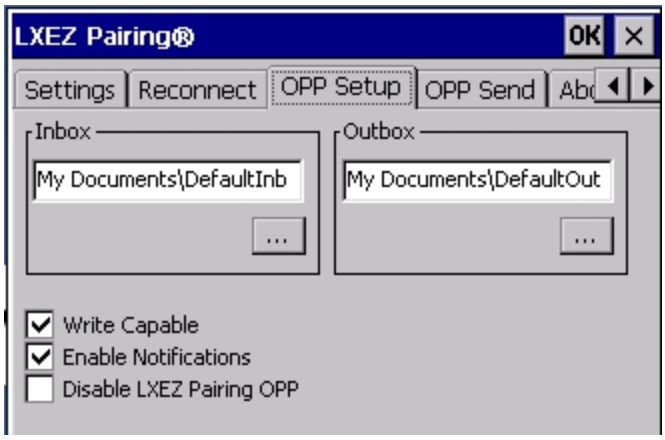
Options

Option	Function
Report when connection lost	This option is Enabled (checked) by default. There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the ok button to remove the dialog box from the screen.
Report when reconnected	This option is Disabled (unchecked) by default. There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the ok button to remove the dialog box from the screen.
Report failure to reconnect	This option is Enabled (checked) by default. The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed. Tap the X button or ok button to close the dialog box. Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.

Option	Function
Clear Pairing Table on Boot	This option is Disabled (unchecked) by default. When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected. When enabled (checked) "Auto Reconnect on Boot" is automatically disabled (dimmed).
Auto Reconnect on Boot	This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence. When disabled (unchecked), no devices are reconnected upon any reboot sequence.
Auto Reconnect	This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior. • When Auto Reconnect is disabled (unchecked), *Auto Reconnect on Boot* is automatically disabled and dimmed. • When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of *Auto Reconnect on Boot* is ignored and no devices are reconnected on boot. The status of *Clear Pairing Table on Boot* controls whether the pairing table is populated on boot. • When Auto Reconnect is enabled (checked) and *Auto Reconnect on Boot* is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). • When Auto Reconnect is enabled (checked) and *Clear Pairing Table on Boot* is enabled (checked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of *Auto Reconnect on Boot* is ignored and the option is automatically disabled (unchecked) and dimmed.

OPP Setup

Use this screen to setup the HX2 for Object Push Protocol (OPP).



Option	Information
Inbox	This is an alphanumeric field displaying the currently selected Inbox. • The Inbox is the location where files pushed to the HX2 from a remote client are stored. Use the browse button **...** to browse to and select the Inbox folder. • Use Windows Explorer to create a custom directory, if desired, before selecting the Inbox folder. • The default Inbox is \My Device\My Documents\DefaultInbox.
Outbox	This is an alphanumeric field displaying the currently selected Outbox. • The Outbox is the location where files are stored to be pushed from the HX2 to a remote server. Use the browse button **...** to browse to and select the Outbox folder. • Use Windows Explorer to create a custom directory, if desired, before selecting the Outbox folder. The default Inbox is \My Device\My Documents\DefaultOutbox.
Write Capable	When checked, files may be written to the HX2. When unchecked, inbound files are rejected. This option is enabled (checked) by default.
Enable Notifications	When checked, the user is notified and may be prompted for a response when files are received by the HX2. When unchecked, inbound files are received with no notification to and no required action from the user. This option is enabled (checked) by default.
Disable LXEZ Pairing OPP	When checked, OPP is disabled in LXEZ Pairing. When unchecked, OPP is enabled in LXEZ Pairing. The default is unchecked, OPP is enabled for LXEZ Pairing. • Because only one application can use OPP at a given time, custom applications should disable OPP in LXEZ Pairing via an API call while the application is using OPP and restore this setting upon completion. • When this item is checked, the other parameter settings on this screen are unavailable (dimmed).

See "Using OPP" on page 101

OPP Send

If LXEZ Pairing OPP is disabled, no file names or OPP servers are displayed on this tab. These areas are grayed out. Similarly the buttons on this tab are also inactive when LXEZ Pairing OPP is disabled.

Option	Information
Send Selected File From Outbox	This area displays the file listing from the currently selected Outbox. All files are shown (*.*). The most recently pushed file is highlighted, assuming that file is still present in the Outbox.
Select OPP Server from Remote Device List	This list displays the known OPP capable servers that the HX2 has previously discovered. The most recently paired server is selected and highlighted.

Buttons

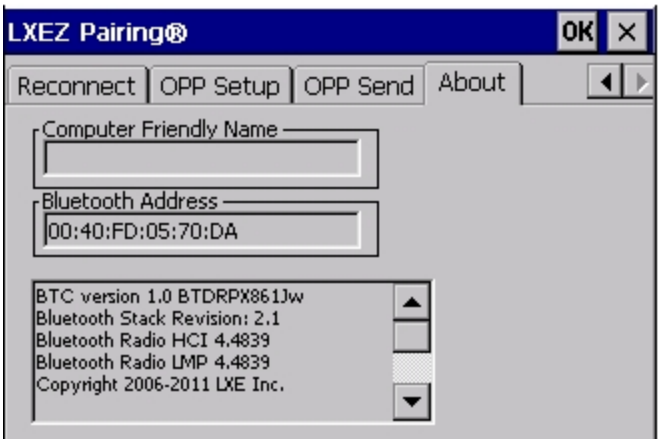
Send - Tapping this button sends (pushes) the selected file to the remote (server) device.

Cancel - Tapping this button cancels the send process initiated by tapping the **Send** button.

Discover - Tapping this button initiates a discovery of OPP devices. Results of the discovery are shown in the OPP Server selection box.

See "Using OPP" on page 101

About



This panel lists the assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth MAC address, and software version levels. The data cannot be edited by the user.

Using Bluetooth

Start | Settings | Control Panel | Bluetooth or Bluetooth icon in taskbar or Bluetooth icon on desktop

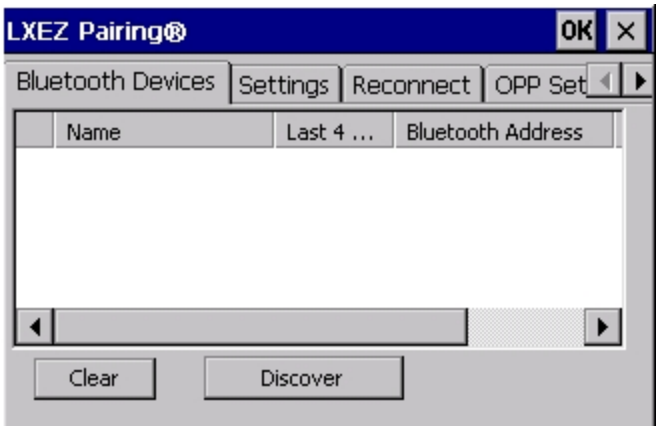
 or  Bluetooth taskbar icon

The HX2 default Bluetooth setting is Enabled.

The LXE HX2 Bluetooth® module is designed to Discover and pair with nearby Bluetooth devices.

Prerequisite: The Bluetooth devices have been setup to allow them to be "Discovered" and "Connected/Paired". The System Administrator is familiar with the pairing function of the Bluetooth devices.

Bluetooth Devices Display - Before Discovering Devices



Initial Configuration

1. Select **Start | Settings | Control Panel | Bluetooth** or tap the Bluetooth icon in the taskbar or on the desktop.
2. Tap the **Settings** Tab.
3. Change the **Computer Friendly Name** at the bottom of the Settings display. The Bluetooth HX2 default name is determined by the factory installed software version. LXE strongly urges assigning every HX2 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the HX2 Bluetooth options on the **Settings** and **Reconnect** tabs.
5. Tap the OK button to save your changes or the X button to discard any changes.

Subsequent Use

Note: Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. A taskbar Bluetooth icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

1. Tap the **Bluetooth icon** in the taskbar or on the desktop to open the Bluetooth LXEZ Pairing application.
2. Tap the Bluetooth **Devices** tab.
3. Tap the **Discover** button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth **Devices** window.
5. **Highlight** a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap **Pair as Scanner** to set up the HX2 to receive scanner data.
7. Tap **Pair as Printer** to set up the HX2 to send data to the printer.
8. Tap **Serial Device** (when Filtered mode is disabled) to set up the HX2 to communicate with a Bluetooth serial device.
9. Tap HID Device to pair a HID device.
10. Tap PAN Device to pair a PAN device.
11. Tap DUN Device to pair a DUN device.
12. Tap **Disconnect** to stop pairing with the device. Once disconnected, tap **Delete** to remove the device name and data from the HX2 Bluetooth Devices list. The device is deleted from the list after the OK button is clicked.
13. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the HX2 display.
14. Whenever the HX2 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the HX2. If the devices cannot connect to the HX2 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

Bluetooth Indicators

The Bluetooth taskbar Icon state and Bluetooth LED state change as Bluetooth devices are discovered, paired, connected and disconnected.

There may be audible or visual signals as paired devices re-connect with the HX2.

Taskbar Icon	Legend
	HX2 is connected to one or more of the targeted Bluetooth device(s).
	HX2 is not connected to any Bluetooth device. HX2 is ready to connect with any Bluetooth device. HX2 is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the HX2 Bluetooth scan range, the Bluetooth connection between the paired device and the HX2 is lost. There may be audible or visual signals as paired devices disconnect from the HX2.

Bluetooth LED	Legend
Blue, blinking slowly	Bluetooth is active but not connected to a device.
Blue, blinking medium	Bluetooth is paired and connected to a device.
Blue, blinking fast	Bluetooth is discovering other Bluetooth devices.
Off	Bluetooth hardware has been turned off or does not exist in theHX2.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the HX2 while AppLock is in control.

Bluetooth Barcode Reader Setup

Please refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Contact your LXE representative for Bluetooth product assistance.

LXE supports several different types of barcode readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the HX2 using Bluetooth functions.

Prerequisites

- The HX2 has the Bluetooth hardware and software installed. An operating system upgrade may be required. Contact your LXE representative for details.
- If the HX2 has a Bluetooth address identifier barcode label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The HX2 main battery is fully charged. Alternatively, the HX2 may be in a powered cradle or cabled to AC/DC power.
- ***Important**: The barcode numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.*
- To open the LXEZ Pairing program, tap **Start | Settings | Control Panel | Bluetooth** or tap the Bluetooth icon on the desktop or tap the Bluetooth icon in the taskbar.

Sample Bluetooth Address Barcode Label

Locate the barcode label, similar to the one shown above, attached to the HX2. The label is the Bluetooth address identifier for the HX2.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

Important: The HX2 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth barcode readers.

HX2 with Label

If the HX2 has a **Bluetooth address barcode label** attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the HX2, with the LXE Bluetooth mobile scanner.
2. If this is the first time the Bluetooth mobile scanner has scanned the HX2 Bluetooth label, the devices are paired. See section titled "Bluetooth Beep and LED Indications". If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel (Start | Settings | Control Panel | Bluetooth).
4. Tap **Discover.** Locate the Bluetooth scanner in the Discovery panel.
5. Double-tap the stylus on the Bluetooth **mobile device** in the list. The right-mouse-click menu appears.
6. Select **Pair as Scanner** to pair the HX2 with the Bluetooth mobile scanner.

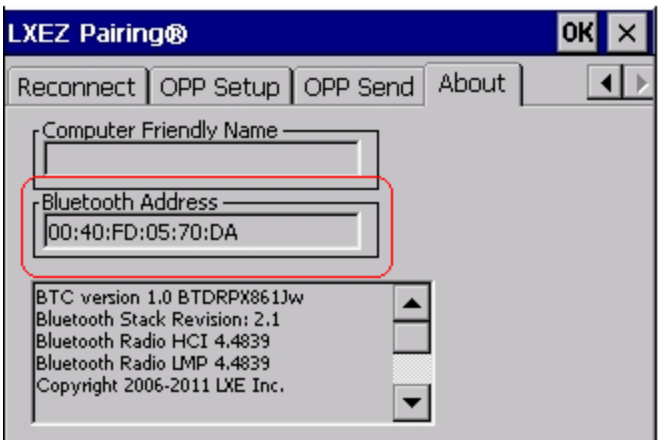
The devices are paired. The Bluetooth mobile barcode reader responds with a series of beeps and an LED flashes. Refer to the following section titled "Bluetooth Beep and LED Indications".

Note: After scanning the HX2 Bluetooth label, if there is no beep and no LED flash from the Bluetooth mobile device, the devices are currently paired.

HX2 without Label

If the HX2 Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the HX2:

First, locate the HX2 Bluetooth address by tapping Start | Settings | Control Panel | Bluetooth | About tab.



Next, create[1] a Bluetooth address barcode label for the HX2.

The format for the barcode label is as follows:

- Barcode type must be Code 128.
- FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, LnkB0400fd002031.

Create and print the label.

Scan the HX2 Bluetooth address barcode label with the Bluetooth barcode reader.

The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes.

Note: After scanning the HX2 Bluetooth label, if there is no beep and no LED flash from the Bluetooth barcode reader, the devices are currently paired.

See "Bluetooth Beep and LED Indications" on page 100

[1] Free barcode creation software is available for download on the World Wide Web. Search using the keywords “barcode create”.

Bluetooth Beep and LED Indications

Beep Type from Bluetooth Device	Behavior
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

LED on Bluetooth Device	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact your LXE representative or LXE Customer Support for assistance.

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible, in direct line of sight, with the HX2 during the pairing process.

1. Open the LXEZ Pairing Panel.
2. Tap **Discover**. Locate the Bluetooth printer in the Discovery panel.
3. Tap and hold the stylus (or doubletap) on the Bluetooth printer ID until the right-mouse-click menu appears.
4. Select **Pair as Printer** to pair the HX2 with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer may respond with a series of beeps or LED flashes.

Please refer to the Bluetooth managed printer manufacturer's User Guide; it may be available on the manufacturer's web site. Contact your LXE representative for Bluetooth product assistance.

Note: If there is no beep or no LED flash from the Bluetooth managed printer, the HX2 and the printer are currently paired.

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of range and then returned within range. See "Reconnect" on page 90

Note: Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the HX2 while AppLock is in control.

Using OPP

Pairing with an OPP Device

Prerequisites

- A remote device, such as a mobile phone, that supports OPP.
- OPP is enabled on the LXE device.

How To

1. Place the remote device in discovery or visible mode.
2. Initiate discovery on the HX2 by tapping the **Discover** button on the **OPP Send** tab.
3. The HX2 discovers the remote device.
4. The HX2 attempts to send a file to the remote device.
5. The remote device prompts the user for a 4 digit PIN.
6. User enters the PIN.
7. The HX2 prompts the user for a 4 digit PIN.
8. User must enter the *same* PIN code as entered on the remote device.
9. The HX2 now pairs with the remote device.

Remote Device Pushes File to HX2

This section assumes that a device supporting OPP is paired with the HX2.

If a duplicate filename is received, LXEZ Pairing writes the file in the specified location, with an incremental number appended to the file name. For example, if a file named **file.jpg** is pushed to the HX2 and that filename already exists in the Inbox, LXEZ Pairing saves the new file as **file001.jpg**. If the same file is pushed again, it is saved as **file002.jpg**.

There are several scenarios based on configuration options on the **OPP Setup** tab.

Notifications enabled, HX2 is Write Capable

1. The OPP client initiates a connection to the HX2 by selecting a file to push to the HX2.
2. The HX2 user is notified that a File Push request has been issued from a remote device.
3. The HX2 user is prompted to accept or reject the incoming request.
4. If the user accepts the request:
    a. The file is pushed to the HX2.
    b. LXEZ Pairing notifies the user that a file has been received.
    c. The connection is closed by the remote device (OPP client).
5. If the user rejects the request:
    a. The file is not pushed to the HX2.
    b. The connection is closed.

Notifications enabled, HX2 is not Write Capable

1. The OPP client initiates a connection to the HX2 by selecting a file to push to the HX2.
2. The file is rejected silently (no notification to the HX2 user).

Notifications disabled, HX2 is Write Capable

1. The OPP client initiates a connection to the HX2 by selecting a file to push to the HX2.
2. The file is accepted silently (no notification to the HX2 user).

Notifications disabled, HX2 is not Write Capable

1. The OPP client initiates a connection to the HX2 by selecting a file to push to the HX2.
2. The file is rejected silently (no notification to the HX2 user).

HX2 Pushes File to Remote Device

This section assumes that a device supporting OPP is paired with the HX2.

The HX2 (OPP client) initiates a connection to the remote device (OPP server) by selecting a file to push to the remote device. The HX2 sends the file and disconnects. The remote device may prompt the user (of that remote device) to accept the incoming request depending on the security settings of the remote device. The prompt may be displayed more than once, or it may not be displayed at all.

Notifications enabled

The file is pushed to the remote device and the user of the HX2 is notified of the completion of the push.

Notifications disabled

The file is pushed to the remote device and the user of the HX2 is not notified of the completion of the push.

LXEZ Pairing and External Application

Because only one application can use the OPP service at a time, external applications that wish to use OPP should disable LXEZ Pairing OPP before using the OPP service and restore LXEZ Pairing OPP upon completion using available API calls (see the *CE API Programming Guide* for details). These API calls are the equivalent of checking or unchecking the Disable LXEZ Pairing OPP checkbox.

- If Disable LXEZ Pairing OPP is not checked, checking it causes LXEZ Pairing OPP to be disabled and the send and receive functionality is disabled.
- If Disable LXEZ Pairing OPP is checked, and no application has registered a callback, un-checking LXEZ Pairing OPP enables OPP functionality in LXEZ Pairing, and the send and receive functionality is enabled.
- If Disable LXEZ Pairing OPP is checked, and another application has registered a callback, un-checking Disable LXEZ Pairing OPP issues a dialog box which says "Another application is using OPP. Do you wish to force their disconnection? Doing so will force the other application to be unregistered." The application that has been forcibly unregistered receives a FORCED_UNREGISTER_RECEIVED event.

Certificates

Start | Settings | Control Panel | Certificates

Manage digital certificates used for secure communication.

Note: Digital certificates are date sensitive. If the date on the HX2 is incorrect, wireless authentication will fail.

The Certificates stores lists the certificates trusted by the HX2 mobile device user.

These values may change based on the type of network security resident in the client, access point or the host system.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

Tap the ? button and follow the instructions in the Windows CE Help file when working with trusted authorities and digital certificates.

Date / Time

Start | Settings | Control Panel | Date/Time - or - Time in Desktop Taskbar

Use this HX2 panel to set Date, Time, Time Zone, and assign a Daylight Savings location.

Factory Default Settings

Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled

There is very little functional change from general desktop or laptop Date/Time Properties options.

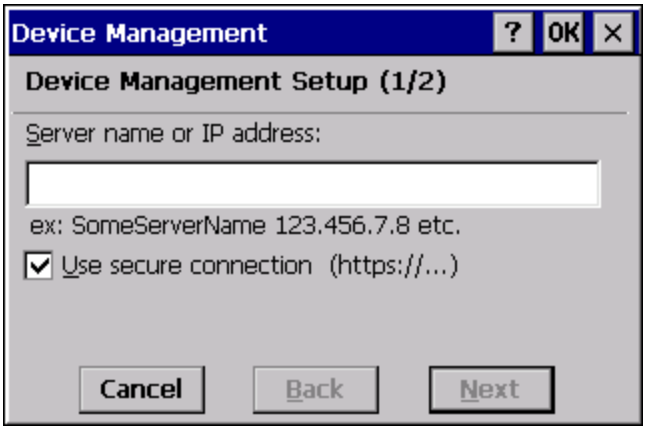
Double-tapping the time displayed in the Desktop Taskbar causes the Date/Time Properties screen to appear.

The Sync button activates a utility that will set the clock using a network time server.

Device Management

Start | Settings | Control Panel | Device Management

Allows a Device Management client (the device equipped with a Microsoft Windows CE operating system) to work with a Microsoft Systems Management Server.



Specify the server name or IP address of the management server and check the checkbox if a secure connection is to be used.

Refer to the Microsoft.com website for more information on device management for Windows CE equipped devices.

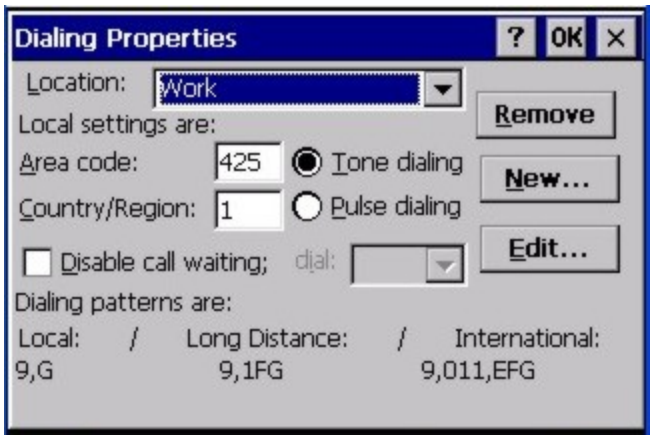
Dialing

Start | Settings | Control Panel | Dialing

Set dialup properties for internal modems (not supplied or supported on the HX2 by LXE).

Factory Default Settings

Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled (blank)



Display

Start | Settings | Control Panel | Display

The display might also called the touchscreen.

Select the desktop background image and appearance scheme for the HX2. Using the options on the Backlight tab, set the display backlight and keypad backlight timers when running on battery or external power.

Adjust the settings and tap the OK button to save the changes. Saved changes take effect immediately.

Factory Default Settings

Background	
Image	Windows CE
Image on background	Disabled
Appearance	
Schemes (color displays)	Windows Standard
Schemes (monochrome displays[1])	High Contrast White
Backlight	
Battery power and user idle	3 seconds
Battery power and System idle	15 seconds
Battery power, idle, Suspend	5 minutes
External power and user idle	2 minutes
External power and System idle	2 minutes
External power, idle, Suspend	2 minutes

[1] Contact your LXE representative for assistance.

Background

There is very little change from general desktop PC Display Properties / Background options. Select an image from the dropdown list (or tap the Browse button to select an image from another folder) to display on the Desktop, and then tap the OK button to save the change. The change takes effect immediately.

Appearance

There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. The default is High Contrast White for monochrome displays and Windows Standard for color displays. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the display.

Backlight

The backlight settings use the LXE set of default timeouts and is synchronized to the User Idle setting in the Schemes tab in the Power control panel.

When the backlight timer expires, the touchscreen backlight is dimmed, not turned off. When both checkboxes are unchecked, the backlight never turns off (or dims).

Default values are 3 seconds for Battery, 2 minutes for External and both the check boxes are enabled.

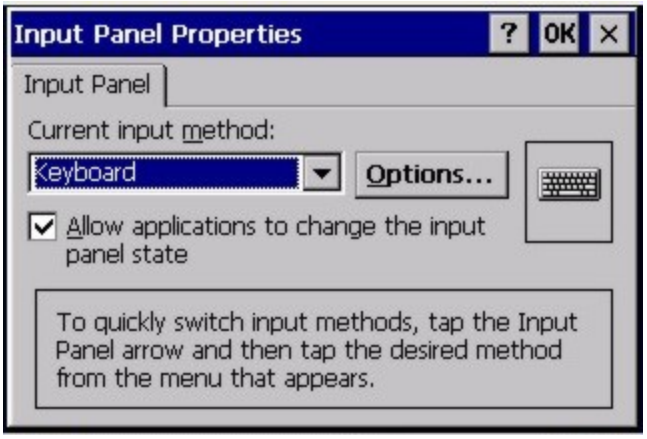
Input Panel

Start | Settings | Control Panel | Input Panel

Set the current HX2 keys and data input method.

Factory Default Settings

Input Method	Keyboard
Allow applications to change input panel state	Enabled
Options button	
Keys	Small keys
Use gestures	Disabled



Use this panel to make the Input Panel (on-screen keyboard) or the physical keypad primarily available when entering data on any screen.

Selecting Keyboard enables both.

Tap the Options button to set the size of the keys displayed on-screen and whether Transcriber gestures are enabled or disabled.

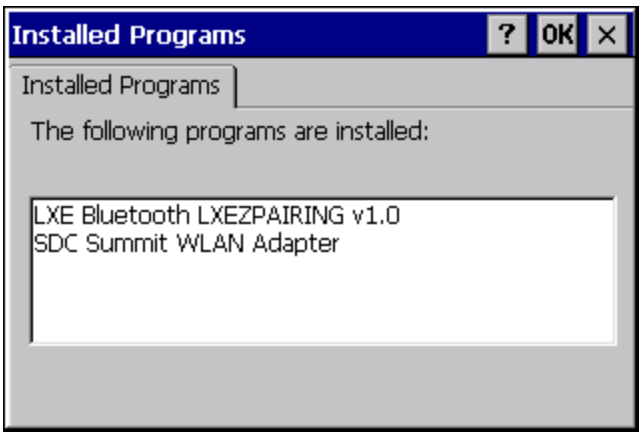
Note: Contact your LXE representative for language packs as they become available.

Installed Programs

Start | Settings | Control Panel | Installed Programs

Note: Lists programs installed in RAM.

View the list of installed programs. No user interaction is required.



Note: Contact your LXE representative for assistance if LXE installed programs must be deleted.

Internet Options

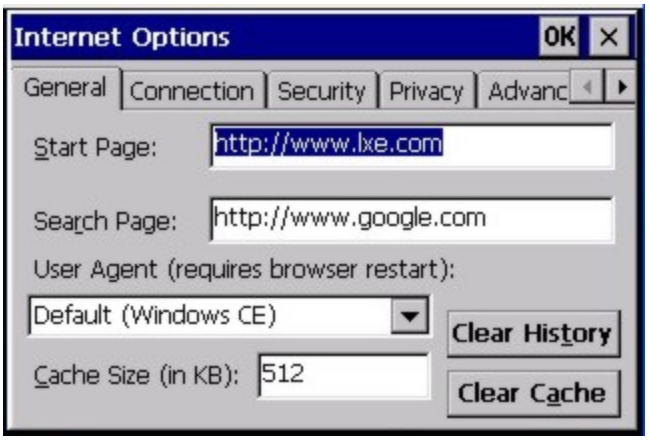
Start | Settings | Control Panel | Internet Options

Set options for HX2 Internet connectivity.

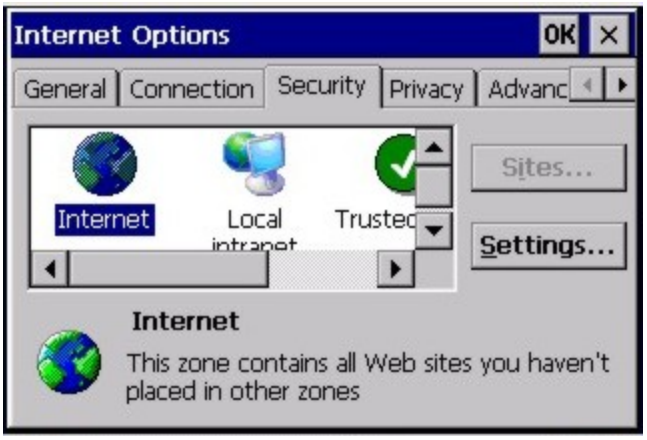
Select a tab. Tap the ? button for help using Windows CE Help installed in your mobile device. Adjust the settings and tap the OK button. The changes take effect immediately.

Factory Default Settings

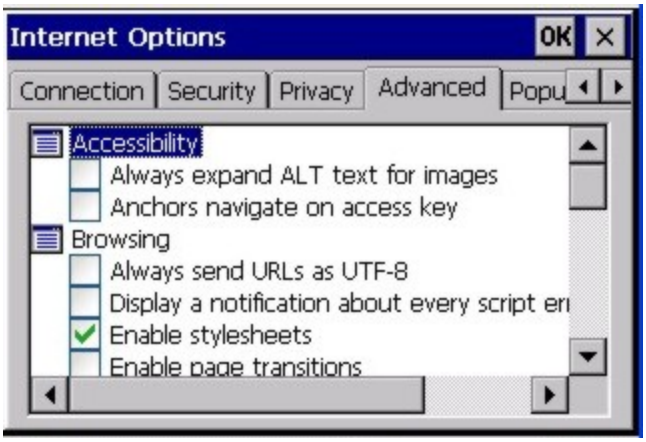
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Bypass Proxy	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Privacy	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced	
Stylesheets	Enabled
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled


Internet Options
OK
General
Connection
Security
Privacy
Advanc
Start Page:
http://www.lxe.com
Search Page:
http://www.google.com
User Agent (requires browser restart):
Default (Windows CE)
Clear History
Cache Size (in KB):
512
Clear Cache


Internet Options
OK
General
Connection
Security
Privacy
Advanc
Use LAN (no autodial)
Autodial name:
USB Client
Network
Access the Internet using a proxy server
Address:
Port:
80
Bypass proxy server for local addresses


Internet Options
OK
General
Connection
Security
Privacy
Advanc
Internet
Local
Trusted
Sites...
Settings...
Internet
This zone contains all Web sites you haven't placed in other zones


Internet Options
OK
General
Connection
Security
Privacy
Advanc
Cookies
First-party
Third-party
Accept
Block
Prompt
Accept
Block
Prompt
Always allow session cookies


Internet Options
OK
Connection
Security
Privacy
Advanced
Popu
Accessibility
Always expand ALT text for images
Anchors navigate on access key
Browsing
Always send URLs as UTF-8
Display a notification about every script er
Enable stylesheets
Enable page transitions


Internet Options
OK
Security
Privacy
Advanced
Popups
Popup Windows
Block popups
Exceptions...
Advanced
Display notification when a popup has been blocked
Open new pages in the current window

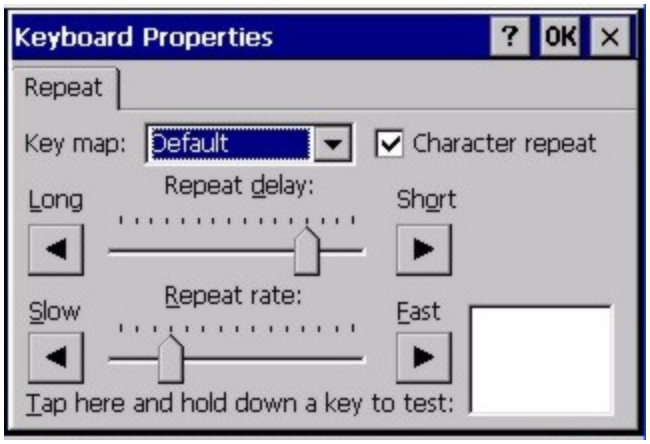
Keyboard

Start | Settings | Control Panel | Keyboard

Set keypad key map, keypad key repeat delay, and key repeat rate.

Factory Default Settings

Repeat Tab	
Key map	Default (or Default HX2)
Repeat character	Enable
Repeat Delay	Short
Repeat Rate	Slow



Select a key map using the drop-down list. Adjust the character repeat settings and tap the OK button to save the changes.

When new key maps, or fonts, are added to the registry, they are available immediately and the font name is in the Keyboard Properties Key map dropdown list. Only one font at a time can be selected. The fonts affect the screen display, they do not affect any virtual (touchscreen) key taps.

See **About | Software | Language** tab for the name of any installed fonts.

Languages and Fonts

Fonts are available in the following languages (in separate part numbers) for each language: Simplified Chinese, Traditional Chinese, Korean, Japanese. Tahoma font is on every unit and includes English (default), European (French, Spanish, German, Portuguese), Scandinavian languages, Arabic, Cyrillic, Greek, Hebrew, and Thai.

See Also: Regional Settings for instruction for setting User Interface Language and Default Input Language.

KeyPad

Start | Settings | Control Panel | KeyPad Icon

Use this control panel option to assign key functions to mappable keys available on your HX2, determine application launch sequences and program command Run sequences.

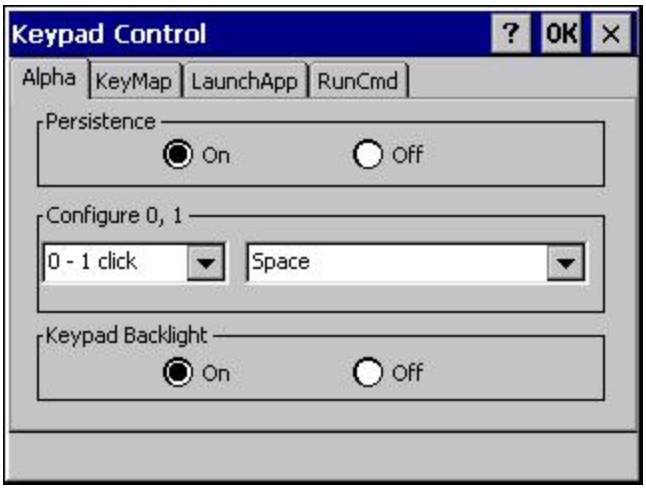
Note: KeyPad Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option.

Factory Default Settings

Alpha (Alpha is not available on the HX2 with a Dual Alpha or Triple Tap keypad)		
Persistence	On	
Configure 0, 1	0 – 1 click	Configure to – Space
Keypad Backlight	On	
KeyMap		
Modifier Mode	None	
Key	Backspace	Remap to – Backspace
Edit String	Field Exit	String – Empty
LaunchApp		
App1	Empty	
App2	Empty	
App3	Empty	
App4	Empty	
App/Opt	EXE	
RunCmd		
Cmd1	Empty	
Cmd2	Empty	
Cmd3	Empty	
Cmd4	Empty	
File/Parm	FILE	

Alpha Tab

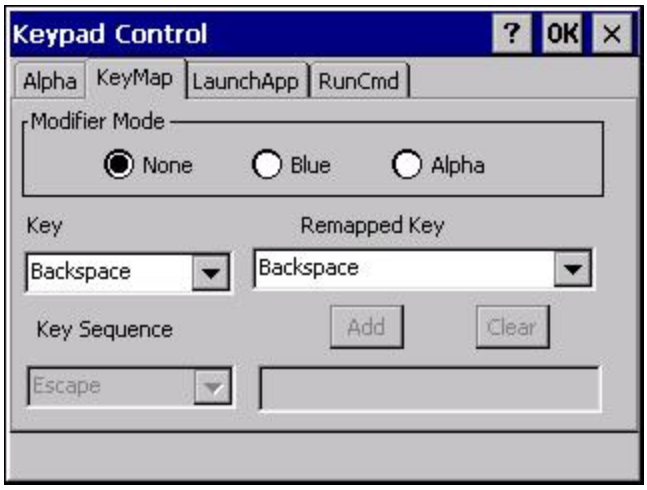
Note: Alpha tab is not available when the HX2 has a Dual Alpha or Triple Tap keypad.



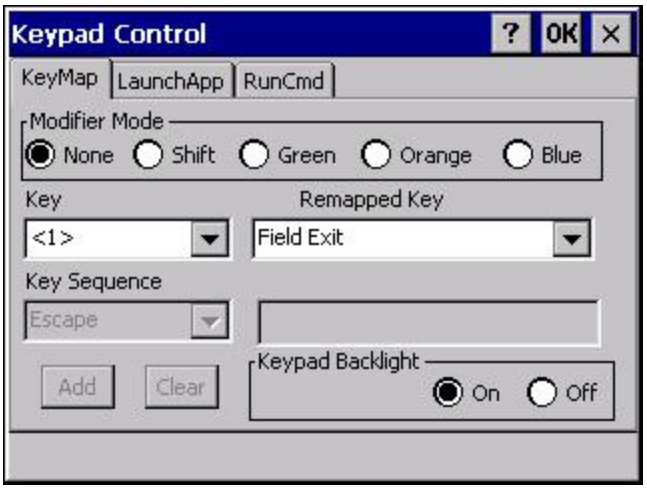
Assign settings by clicking radio buttons and selecting keys from the drop down boxes.

Persistence	Select the Off radio button (disable) when the Alpha key is to be tapped every time an alpha character is desired. The default value is On (enabled).
Configure 0, 1	Use the drop down boxes to assign a specific number of keyclicks, of either the 0 or 1 key, to map another key command to the 0 or 1 key sequence. The same key command can be assigned to more than one 0 or 1 keyclick sequence.
Keypad Backlight	Select the Off radio button (disable) when the keypad backlight is to remain Off regardless of the OS event in process. The default value is On (enabled). When On the keypad backlight responds to OS events as designed. When On, keypad backlight behavior is based on the settings of the Display Backlight Timer.

KeyMap Tab



Alpha Mode 3 Tap Keypad



Dual Alpha or Triple Tap Keypad

Assign settings by clicking radio buttons and selecting keys from the drop down boxes. Tap the OK button when finished. The changes take effect immediately.

How to Remap a Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select the value from the remapped key from the Remapped Key pulldown list.
4. Click OK to save the result and close the Keypad Control.

How to Remap a Key Sequence

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Key Sequence from the Remapped Key pulldown list.
4. Select the first key for the multiple key sequence from the pulldown list. Press the Add button to add the key to the multiple key sequence shown in the Key Sequence box. Repeat this step until all keys desired have been added to the key sequence. If necessary, use the Clear button to erase all entries in the Key Sequence box.
5. Click OK to save the result and close the Keypad Control.

Note: A key can only be used once in a multiple key sequence. For example, an F1 key added to a key sequence means an F1 key cannot be used again in the same key sequence.

How to Remap an Application

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Launch App1-4 from the remapped key from the Remapped Key pulldown list.
4. Click on the LaunchApp tab.
5. Make sure the EXE radio button is selected.
6. In the text box (App1-4) corresponding to the number selected for Launch App1-4, enter the application to launch.
7. If any parameters are needed for the application, click on the OPT radio button. This clears the text box (though the application name is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the Keypad Control.

9. If the KeyMap tab is accessed again, the application plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

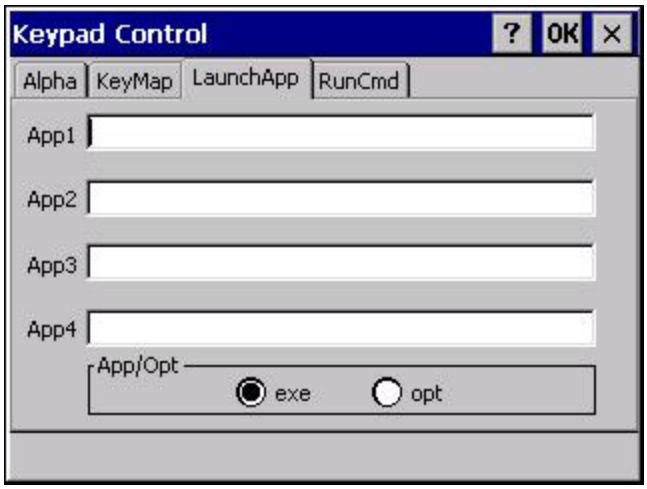
How to Remap a Command

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select RunCmd 1-4 from the remapped key from the Remapped Key pulldown list.
4. Click on the RunCmd tab.
5. Make sure the FILE radio button is selected.
6. In the text box (Cmd1-4) corresponding to the number selected for RunCmd1-4, enter the desired command.
7. If any parameters are needed for the command, click on the PARM radio button. This clears the text box (though the command is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the Keypad Control.
9. If the KeyMap tab is accessed again, the command plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

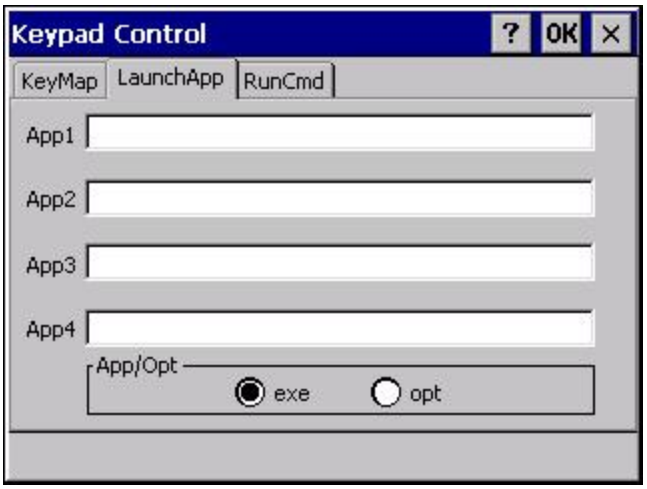
LaunchApp Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the HX2 emits a single beep, if the launch is successful, it is silent.



Alpha Mode 3 Tap Keypad



Dual Alpha or Triple Tap Keypad

The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g. App1, App2.
2. Enable the EXE radio button if the application is an EXE file.
3. Enter the name of the executable file.
4. Enable the OPT radio button to add options or parameters for the executable file in the same text box. Switching from EXE to OPT clears the text box (but the information previously entered is stored), allowing parameter entry.

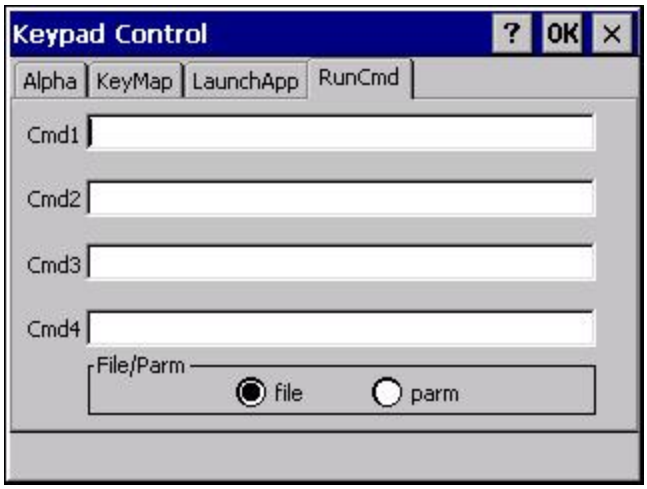
Tap the OK button when finished. The changes take effect immediately.

The result of the application (exe) and options (opt) entries are displayed on the KeyMap tab in the Key Sequence box when the key mapped to the LauchApp is selected.

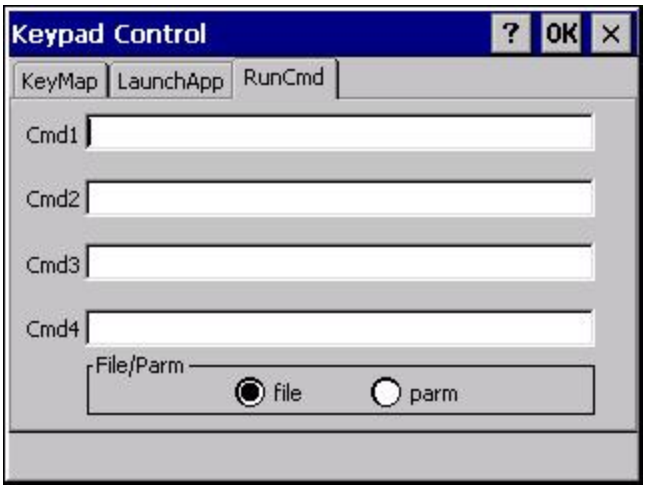
RunCmd Tab

The default for all text boxes is Empty, Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the HX2 emits a single beep, if the launch is successful, the mobile device is silent.



Alpha Mode 3 Tap Keypad



Dual Alpha or Triple Tap Keypad

The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g. Cmd1, Cmd2.
2. Enable the file radio button and enter the name of the file.
3. Enable the PARM radio button to add parameters for file/exe execution in the same text box.

Tap the OK button when finished. The changes take effect immediately.

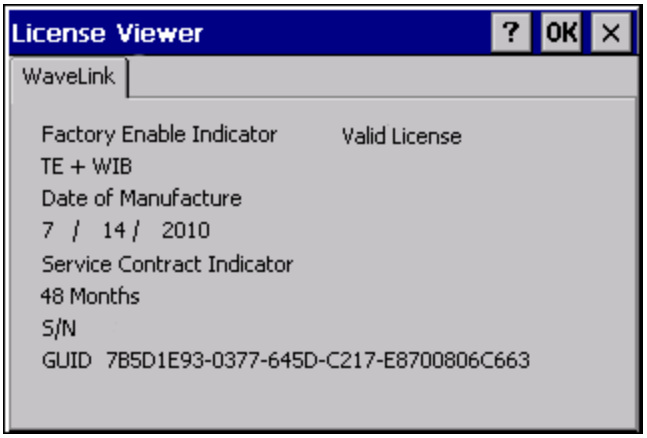
License Viewer

Start | Settings | Control Panel | License Viewer

Use this option to view software license registration details, and service contract length for a HX2. Information on the License Viewer tabs is unique for each HX2.

Note: Following image is an example.

Your License Viewer control panel may show more tabs, e.g. RFTerm, depending on the number of software applications running on the HX2 that require a license. Contact your LXE representative for software updates and releases as they become available.



Software and driver version information is located in the About control panel. Copyright information is located in the System control panel.

Mixer

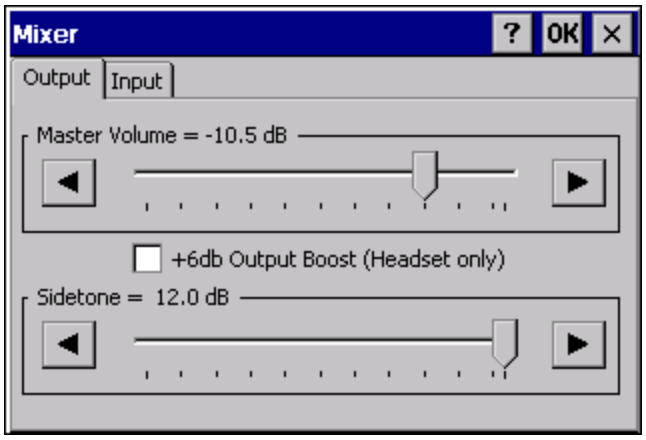
Start | Settings | Control Panel | Mixer

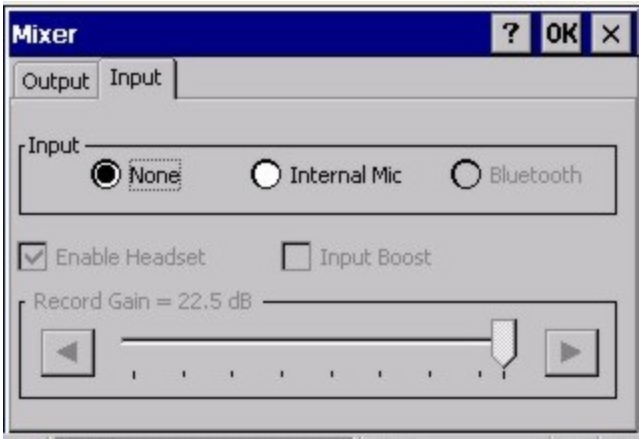
The HX2 has a speaker and a microphone. They are active when a headset is not connected to the device.

The microphone is located to the right of the LXE oval logo at the top of the unit.

Use the settings on these panels to adjust the volume, record gain and sidetone for microphone input, speaker and speaker output.

Headsets can be enabled, disabled and selected using these panels.





Mixer Output

Tap and hold the sliders. Move them either left or right, or tap the left and right arrows, to adjust decibel level.

Output Boost	When checked (enabled) increases the sensitivity of the headset by +6db.

Mixer Input

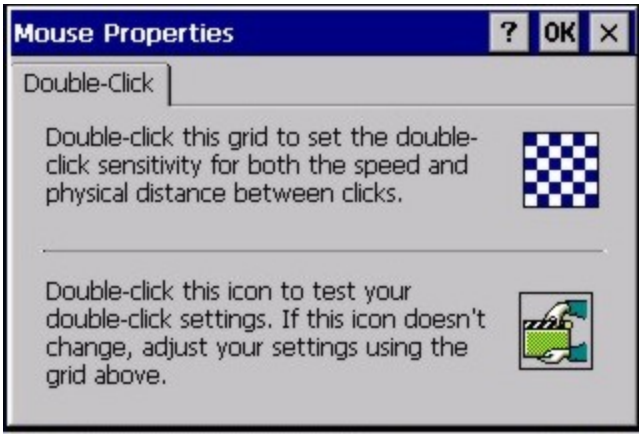
Tap and hold the slider. Move it either left or right, or tap the left and right arrows, to adjust decibel level.

Option	Function
None	When enabled, the internal microphone is turned off. The default is unchecked (disabled).
Internal Mic	When enabled, the internal microphone is turned on. The default is checked (enabled). Enable the Input Boost checkbox to boost Record Gain by 20 dB. For example, if Record Gain is set to 40 dB and Input Boost is enabled, the dB for microphone output is boosted by 20 dB. The resulting microphone output would be approximately 60 dB.
Bluetooth	Future use.
Enable Headset	When Enable Headset is unchecked (disabled), the internal speaker and microphone are enabled. When Enable Headset is checked (enabled), the internal speaker and microphone are disabled. The default is checked (enabled). *When you will be using a tethered battery/audio cable without a headset, disable the Enable Headset parameter.*
Input Boost	When checked (enabled) increases the sensitivity of the microphone (internal or headset) by 20 dB.
Record Gain	Tap and hold the slider and move it left and right to adjust. Or tap the left and right arrow keys to adjust the slider. The default is 22.5 dB.

Mouse

Start | Settings | Control Panel | Mouse

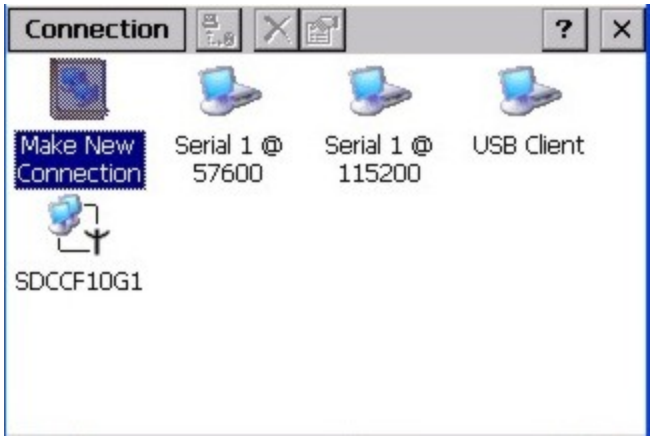
Use this option to set the double-tap sensitivity for stylus taps on the HX2 touchscreen.



Network and Dialup Options

Start | Settings | Control Panel | Network and Dialup Connections

Set HX2 network driver properties and network access properties. Select a connection to use, or create a new connection.



Create a New Connection

1. On the mobile device, select **Start | Settings | Control Panel | Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the connection you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the **Next** button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the Port Settings tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off Wait for dial tone, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap **OK**.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start | Settings | Control Panel | PC Connection** and tap the **Change Connection…** button.
11. Select the new connection. Tap **OK** twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Click the desktop **Connect icon** to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Network Capture

Start | Settings | Control Panel | Network Capture

Note: Verify the date and time before using the logging utilities to ensure meaningful data.

The Network Capture panels provide configuration options for logging utilities.

Two types of logging are configurable:

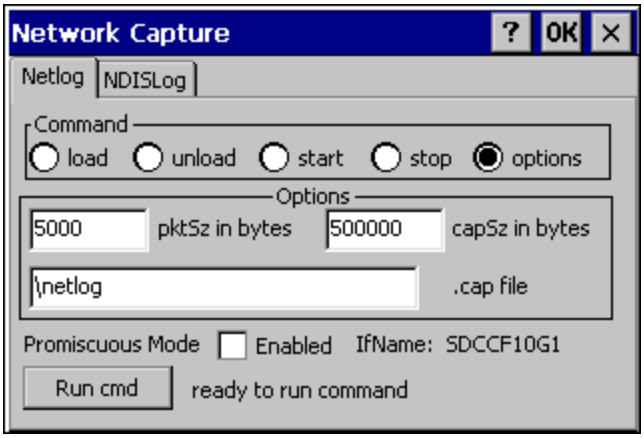
Netlog is a Windows CE utility that monitors network traffic. Netlog creates a .CAP file that can be read using Microsoft Windows Network Monitor or any compatible tool that supports .CAP files.

NDISLog monitors the NDIS interface between the Summit radio and the NDIS driver. This utility creates a .TXT log file.

Factory Default Settings

Netlog	
Command	options
pkt_size in bytes	5000
cap_size in bytes	500000
.cap file	\netlog
Promiscuos Mode	Disabled
NDISLog	
Command	stop
file	\ndislog.txt

Netlog



Use this control panel to configure the Netlog utility. By configuring Netlog using the control panel, Netlog remains running across a warmboot. However, please note that:

- Netlog first stores data to a file named netlog0.cap, then netlog1.cap. Any time the current file reaches maximum size, Netlog switches to the other file.
- If the log file is stored in the root directory, any previous data is lost and a new log file started after the warm.boot
- If the log file is stored in \System, all previous data is saved across the warmboot.
- If Netlog is enabled across the warmboot, a series of brief popups may be displayed during the boot cycle. No user interaction is required.

Command

Command	Function
options	Specifies the option to perform. See the table below for the option parameters and values.
load	Loads and starts Netlog.
start	Starts the Netlog process of logging the network traffic.
stop	Stops Netlog from logging network traffic.
unload	Unloads Netlog.

Options

Options	Function
pkt_size in bytes	Specifies the maximum packet size captured in bytes. This option should only be run after you have called **load** and **stop**. Default is 5000.
cap_size in bytes	Specifies the maximum size of Netlog0.cap or Netlog1.cap in bytes. This option should only be run after you have called **load** and **stop**. Default is 500,000.
.cap file	Specifies the name of the file to which network traffic information is saved. This option should only be run after you have called **load** and **stop**. Default is \netlog.

Run cmd

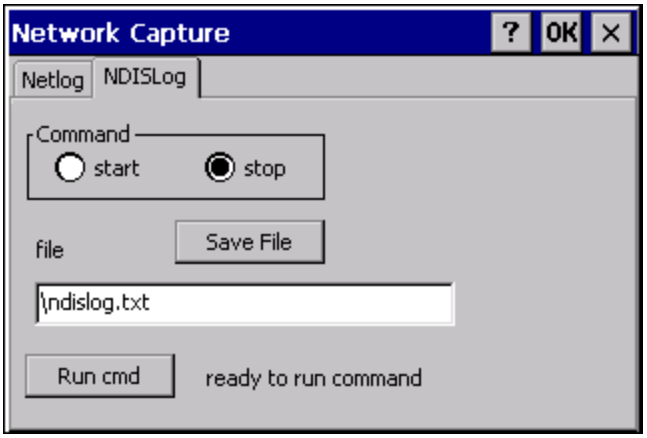
Performs the command selected. For example, to run Netlog and modify the packet size do the following:

Select **load** from the Commands list and click the **Run cmd** button.

Select **stop** from the Commands list and click the **Run cmd** button.

Select **options** from the Commands list, enter the new packet size in the Options list and click the **Run cmd** button.

NDISLog



NDISLog creates a .TXT file that can be viewed with any text editor program that supports .TXT files.

Command

Command	Function
start	Starts logging the network traffic.
stop	Stops logging network traffic.

file

Specifies the name of the file to which NDISLog information is stored.

Save File

Stores the file name.

Run cmd

Performs the selected start or stop command.

HX2-3 Options

Start | Settings | Control Panel | HX2-3 Options

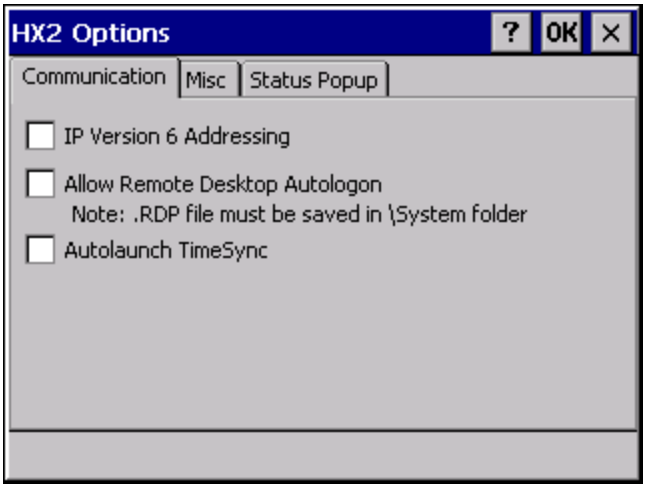
Set options such as IP V6, time sync, touchscreen enable and CapsLock. Also set Status Popup taskbar icon display options for the Admin and User.

It may be necessary to warmboot the HX2 after making desired changes A pop up window indicates if a warmboot is required.

Note: If there is no icon corresponding to this item in the Control Panel, contact your LXE Representative for upgrade details.

Communication

Options on this tab configure communication options for the HX2.



Enable TCP/IP Version 6

By default, IPv6 is disabled on the HX2. Check this checkbox to enable IPv6.

Allow Remote Desktop Autologon

By default, Remote Desktop Autologon is disabled. Check this checkbox to enable Remote Desktop Autologon.

Note: The .RDP file must be saved in the \System folder. When prompted, use the Save As button to save the .RDP file is the \System directry. If the .RDP file is saved in the default root folder location, the .RDP file will not persist across a warmboot.

Autolaunch TimeSync

By default, TimeSync does not automatically run on the HX2. To enable TimeSync to run automatically on the HX2, check this checkbox.

Synchronize with a Local Time Server

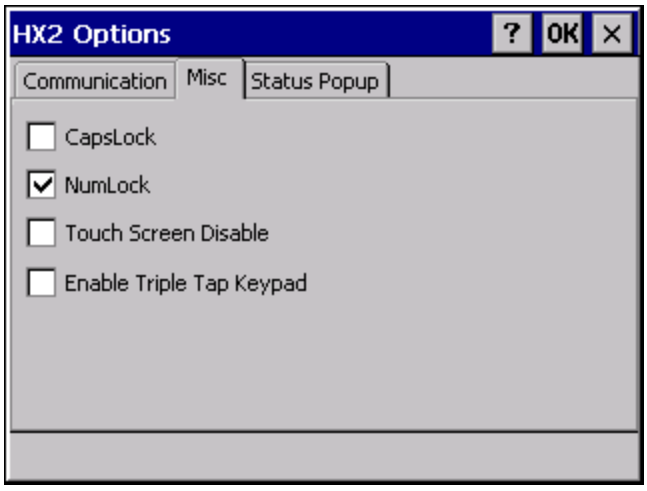
By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy GrabTime.ini from the My Device | Windows folder on the mobile device to the host PC.
2. Edit the copy of GrabTime.ini on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini file to the My Device | System folder on the mobile device.

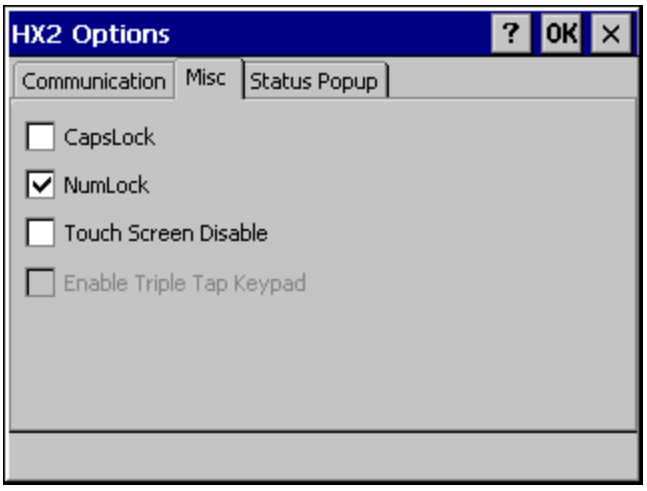
The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Misc

Options on this tab configure device specific options. Note that options not available on the HX2 are dimmed or grayed out.



HX2 Dual Alpha and Triple Tap Keypads



HX2 Alpha Mode 3 Tap Keypad

CapsLock

By default, CapsLock is disabled after a warmboot. To enable CapsLock after a warmboot, check this checkbox.

NumLock

By default, NumLock is enabled after a warmboot. To disable NumLock after a warmboot, uncheck this checkbox.

Touch Screen Disable

By default, the HX2 touchscreen is enabled. To disable the touchscreen after a warmboot, check this checkbox.

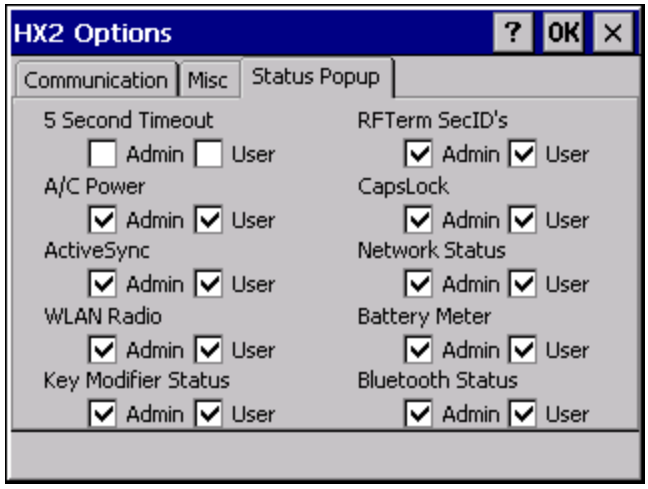
Enable Triple Tap Keypad

This option is not available on the HX2 with the legacy keyboard.

By default, the HX2 is configured for the Dual Alpha style keypad. Check this box to enable the Triple Tap style keypad.

Status Popup

Options on this tab configure the Status Popup window. When the Status popup window is displayed, it is placed on top of the window in focus and hides any data beneath it. It is closed by pressing the assigned Status User or Status Admin key sequence.



Using the key mapping control panel, the System Administrator must first assign a **Status User** key sequence for the end-user when they want to toggle the Status Popup Window on or off.

The System Administrator must also assign a **Status Admin** key sequence to perform the same function. Status popup window display options (taskbar icons) are assigned on the Status Popup tab. E.g. AC Power, ActiveSync, WLAN radio, CapsLock, Network status, Bluetooth status, etc.

The default for the User and Admin status popup windows is to show all status information. The 5 second timeout to remove the status popup from the display is disabled by default for the User and Admin status popup windows.

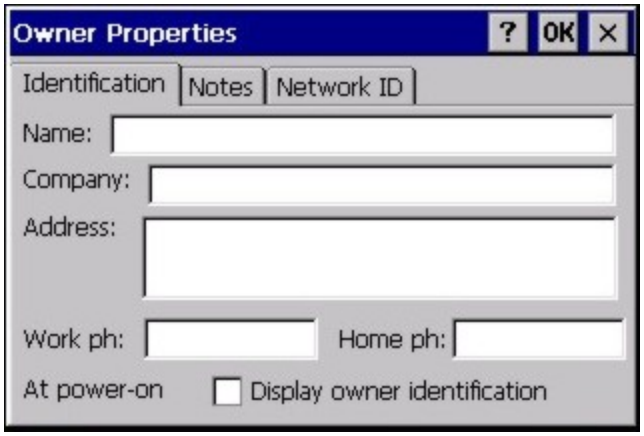
Owner

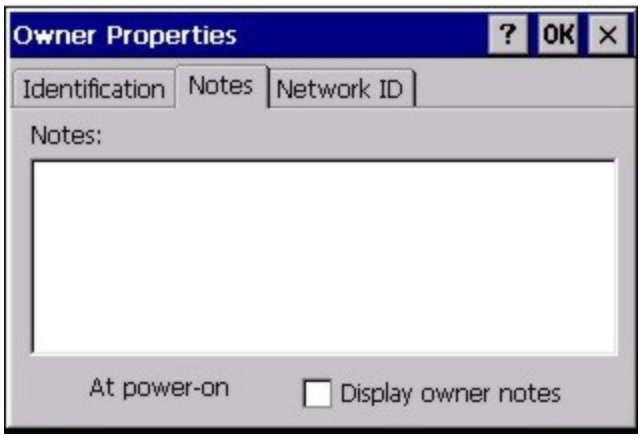
Start | Settings | Control Panel | Owner

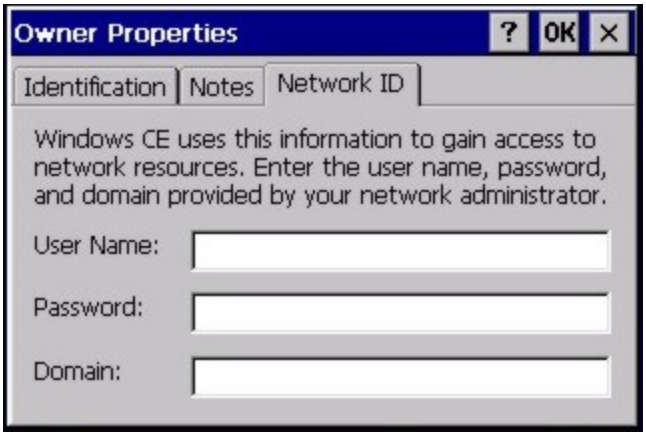
Set the HX2 owner details. The Network ID is used when logging into a remote network.

Factory Default Settings

Identification	
Name	Blank
Company	Blank
Address	Blank
Telephones	Blank
Display owner ID at power-on	Disabled
Notes	
Notes	Blank
Display notes at power-on	Disabled
Network ID	
User Name	Blank
Password	Blank
Domain	Blank







Enter user name, password and domain to be used when logging into network resources.

Password

Start | Settings | Control Panel | Password

Use this panel to set HX2 user access to control panels and power up password properties.

Important: This password must be entered before performing a cold boot or cold reset.

If entering a power-on or screen saver password does not allow you to disable this password protection or perform a cold boot, contact Customer Support.

Factory Default Settings

Password	Blank
Enter password at Power On	Disabled
Enter password at Remote Desktop Screen Saver	Disabled

- The password and password settings are saved during a warm boot and a cold boot.
- The screensaver password affects the Remote Desktop screensaver only.
- After a password is assigned and saved, each time a Settings | Control Panel option is selected, the user will be required to enter the password before the Control Panel will open.
- The screensaver password is the same as the power-on password. They are not set independently.
- A screensaver password cannot be created without first enabling the “Enable password protection at power-on” check-box.
- The screensaver password is not automatically enabled when the “power-on” checkbox is enabled.

Enter the password in the Password text box, then press Tab and type the password again to confirm it.

Enable the power-on checkbox and, if desired, the screensaver checkbox.

A changed/saved password is in effect immediately.

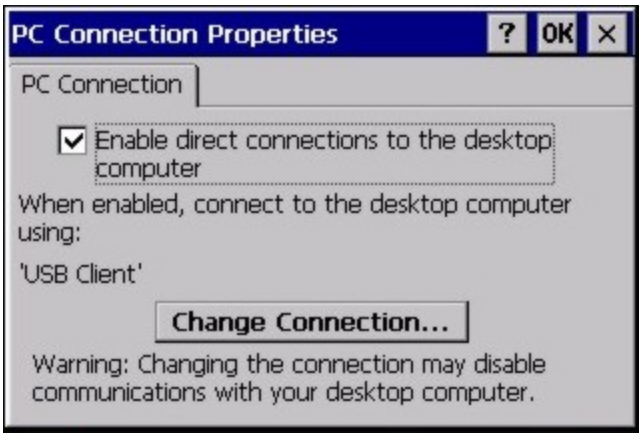
PC Connection

Start | Settings | Control Panel | PC Connection

Use these options to control a cabled connection (USB, serial) between the HX2 and a nearby desktop/laptop computer.

Factory Default Settings

Enable direct connection	Enabled
Connect using	USB Client



Unchecking the **Enable direct connections** checkbox disables ActiveSync on the HX2.

Tap the **Change Connection** button to change the direct connect setting.

Tap the drop-down box to view a list of pre-configured connection settings.

Power

Start | Settings | Control Panel | Power

The HX2 power mode timers are cumulative.

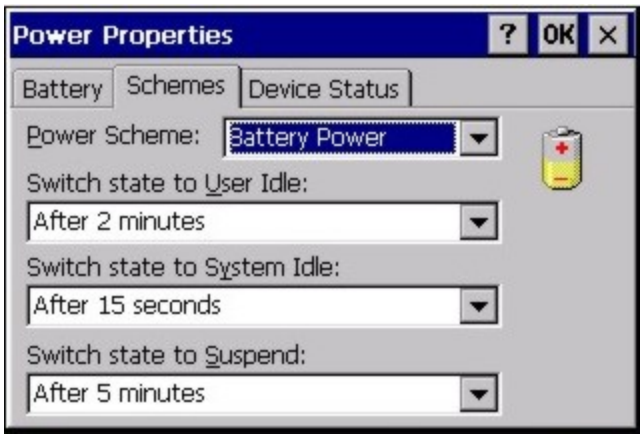
The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired.

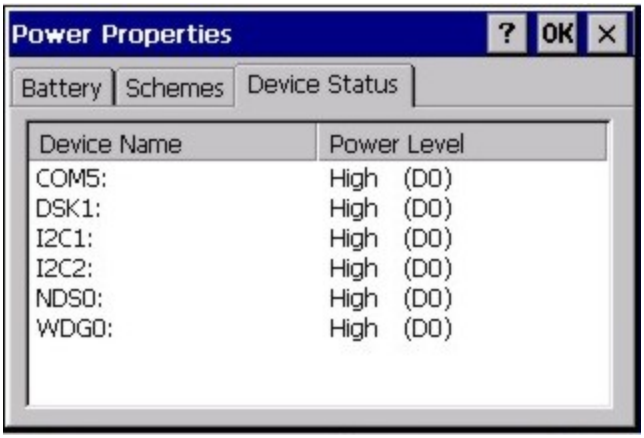
When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

The Display | Backlight setting is synchronized with the User Idle setting in the Schemes tab in the Power control panel.

Factory Default Settings

Battery Tab	
Schemes Tab	
Battery Power - User Idle Timeout	3 seconds
Battery Power - System Idle Timeout	15 seconds
Battery Power - Suspend Timeout	5 minutes
AC Power - User Idle Timeout	2 minutes
AC Power - System Idle Timeout	2 minutes
AC Power - Suspend Timeout	5 minutes
Device Status Tab	No user interaction





Because of the cumulative effect, and using the Battery Power Scheme Defaults listed above:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 sec + 3 sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.

If the User Idle timer is set to Never, the power scheme timers never place the device in User Idle, System Idle or Suspend modes.

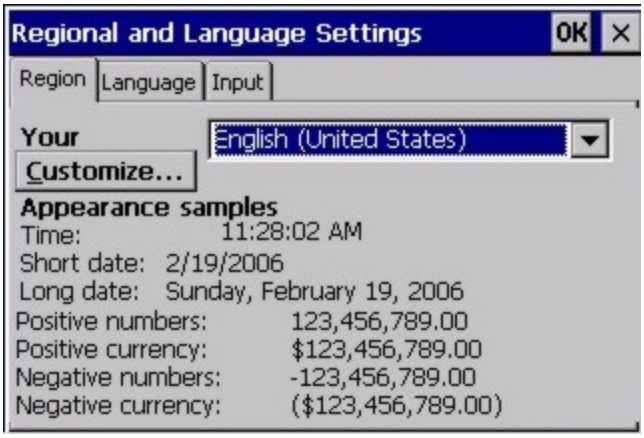
Regional and Language Settings

Start | Settings | Control Panel | Regional Settings

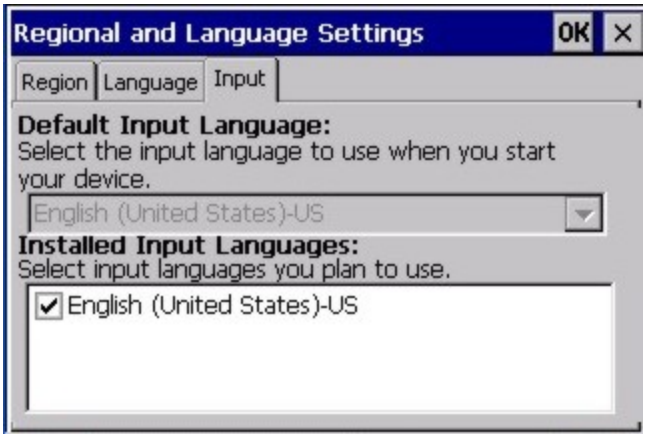
Set the appearance of numbers, currency, time and date based on regional and language settings. Set the HX2 user interface language and the default input language.

Factory Default Settings

Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US




Regional and Language Settings
OK
Region
Language
Input
User Interface Language:
The option will determine the language used for the menus, dialogs and alerts.
English (United States)


Regional and Language Settings
OK
Region
Language
Input
Default Input Language:
Select the input language to use when you start your device.
English (United States)-US
Installed Input Languages:
Select input languages you plan to use.
English (United States)-US

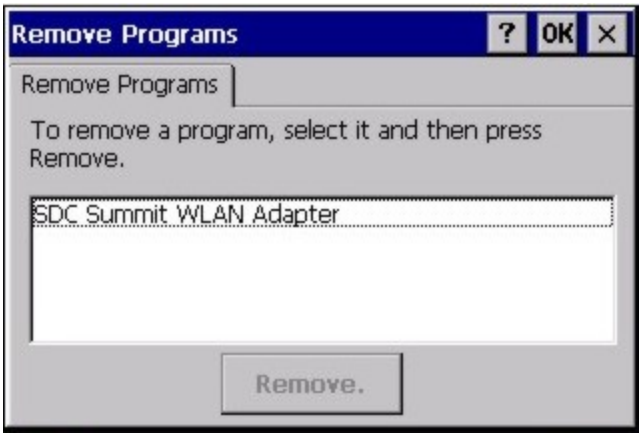
Remove Programs

Start | Settings | Control Panel | Remove Programs

Note: Lists programs installed in RAM that have been marked for removal.

Select a program and tap Remove. Follow the prompts on the screen to uninstall HX2 user-installed only programs. The change takes effect immediately.

Files stored in the **My Documents** folder are not removed using this option.



Note: Do not remove LXE-installed programs using this option. Contact your LXE representative for assistance if LXE installed programs must be deleted.

Scanner Wedge Introduction

Start | Settings | Control Panel | Scanner

Set HX2 scanner keyboard wedge parameters, enable or disable allowed symbologies, scanner icon appearance, active scanner port, and scan key settings.

Assign baud rate, parity, stop bits and data bits for available COM ports.

Parameters on the Main tab and the COM tab(s) apply to this device only.

Barcode manipulation parameter settings on the Barcode tab are applied to the incoming data resulting from successful barcode scans sent to the HX2 for processing. The successful barcode scan data may be sent by

- a wireless Bluetooth Handheld Scanner,
- or a tethered ring scanner.

After hot swapping HX2 ring scanners, the HX2 auto-detects the ring scanner type. The scanner/imager activates when the Scan button on the ring is pressed.

Important: The ring decoders are initialized during HX2 power up by the scanner wedge driver. Every time you scan the Reset to Factory Default barcode in the *Ring Scanner Programming Guide*, select **Start | Settings | Control Panel | Scanner**. After the scanner panel has opened, click OK to close the panel and the ring decoder is initialized.

Barcode Processing Overview

Barcode processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Scanner control panels. The steps are presented below in the order they are performed on the barcode data.

1. Scanned barcode is tested for a **code ID** and matching length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the barcode data is processed based on the settings for All.
2. If symbology is **disabled**, the scan is rejected.
3. Strip **leading** data bytes unconditionally.
4. Strip **trailing** data bytes unconditionally.
5. Parse for, and strip if found, **Barcode Data** strings.
6. Replace any **control characters** with string, as configured.
7. Add **prefix** string to output buffer.
8. If **Code ID** is ***not*** stripped, add saved **code ID** from above to output buffer.
9. Add processed **barcode string** from above to output buffer.
10. Add **suffix string** to output buffer.
11. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
12. If key output is enabled, start the process to output keys. If control characters are encountered:

    - If Translate All is set, key is translated to CTRL + char, and output.
    - If Translate All is not set, and key has a valid VK code, key is output.
    - Otherwise, key is ignored (not output).

The barcode data is ready to be read by applications.

Factory Default Settings

Main Tab	
Port 1	Disabled until auto-detect
Port 2	Ring
Port 3	Disabled until auto-detect
Send Key Message (WEDGE)	Enabled
Enable Scanner Sound	Enabled
Imager LED Illumination	Internal
COM1 Tab (Cradle serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Barcode Tab	
Enable Code ID	None
Continuous Scan Mode	Disabled

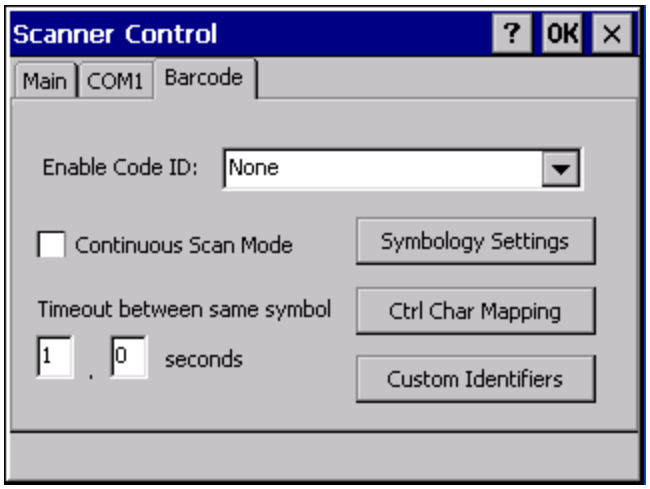
Continuous Scan Mode

Start | Settings | Control Panel | Scanner | Barcode Tab

Enabling Continuous Scan Mode will ensure the laser is always on and decoding.

Caution: Laser beam is emitted continuously. Do not stare into the laser beam.

Set the *Timeout between same symbol* to a value sufficient to prevent the beeper from continuously beeping when a symbol is left in the scanner's field of view.



When the barcode decoder is in continuous mode the scan button functions as an On/Off switch.

The ring decoder red LED will always be off in continuous mode.

The audio beeps and green LED work the same as they do for normal scan mode.

If scan mode, power mode, or timeout between same symbol parameters are changed using external configuration barcodes in the *Ring Scanner Programming Guide*, the HX2 operating system automatically restores the parameters to their programmed settings upon a warm or cold boot and/or any change made in the control panel.

Toggling between continuous and normal scan modes is in effect immediately upon pressing the OK button in this control panel, a warm boot is not required or necessary.

Main Tab

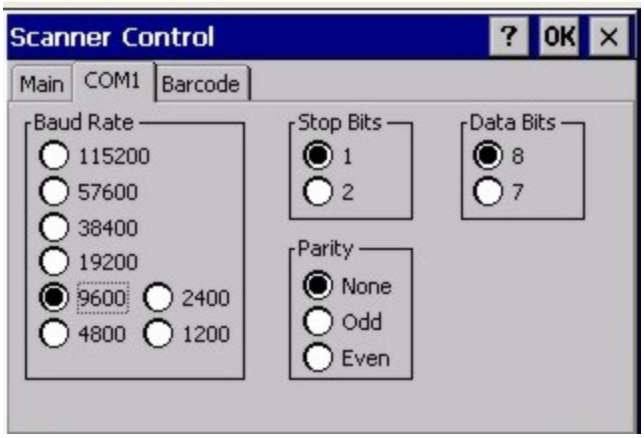
Start | Settings | Control Panel | Scanner | Main tab

Parameter	Function
Port	The ports are disabled until the HX2 auto-detects a device tethered to the port. Port 1 defaults to Bluetooth and Port 2 defaults to Ring when a Bluetooth enabled HX2 with ring scanner/imager is powered On
Send Key Messages (WEDGE)	Default: Enabled. When Send Key Messages (WEDGE) is checked any data scan is converted to keystrokes and sent to the active window. When this checkbox is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using Wedge.
Enable Scanner Sound	Default: Enabled. Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from an external scanner, and then the rejection of scanned barcode data by the processing causes a bad scan beep from the HX2 on the same data.
Imager LED Illumination	The default setting is Internal illumination. The imager has a bank of three LEDs above the imager aperture that illuminate when External or Both radio buttons are enabled. The illumination turns off when the scan is complete.
Single Scan	Options are Off (default), Auto and Man.

Click here to view factory default settings for this panel.

COM1 Tab

Start | Settings | Control Panel | Scanner | COM1



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

This panel does not configure the connected device. Please refer to the documentation for the external connected or wireless device for information on configuring the device.

Note: COM default values are restored after a cold boot or operating system upgrade.

Serial Port Pin 9

COM1 does not support 5V switchable power on pin 9 for handheld serial tethered scanners. Ring scanners are tethered to the HX2. Handheld serial tethered scanners can be connected to the HX2 through the cradle serial port.

Barcode Tab

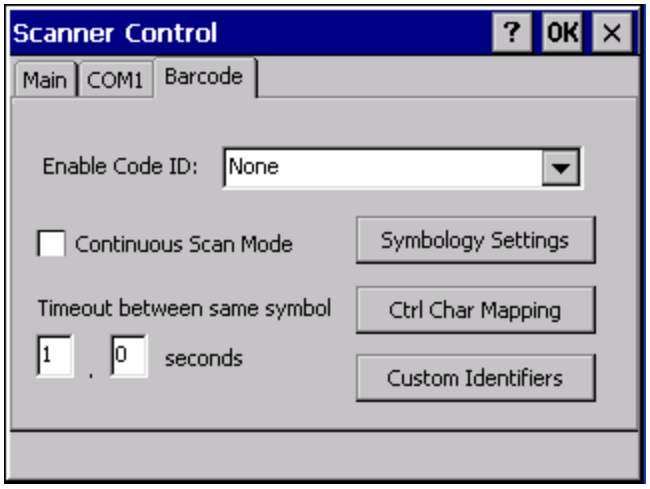
Start | Settings | Control Panel | Scanner | Barcode tab

The Barcode tab contains several options to control barcode processing. Options include:

- Defining custom Code IDs
- Disable processing of specified barcode symbologies
- Rejecting barcode data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified barcode data strings
- Replacing control characters
- Adding a prefix and a suffix.
- When Continuous Scan Mode is enabled, set the *Timeout between same symbol* to a value sufficient to prevent the beeper from continuously beeping when a symbol is left in the scanner's field of view.

Notes:

- The Scanner application (Wedge) can only enable or disable barcode processing inside the Wedge software.
- The Scanner application enables or disables the Code ID that may be scanned.
- Enabling or disabling a specific barcode symbology is done manually using the configuration barcode in the *Integrated Scanner Programming Guide* (available on the LXE Manuals CD and the LXE ServicePass website).



Choose an option in the Enable Code ID drop-down box: None, AIM ID, Symbol ID, or Custom ID.

Buttons

Symbology Settings	Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.
Ctrl Char Mapping	Define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes.
Custom Identifiers	Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

See "Barcode Processing Overview".

Enable Code ID

This parameter programs the scanner to transmit the specified Code ID and/or determines the type of barcode identifier being processed.

Transmission of the Code ID is enabled at the scanner for all barcode symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

Options

- **None:** Programs an internal scanner to disable transmission of a code ID. After clicking the Symbology Settings button, the only entry on the Symbology listing is All, plus any configured custom IDs. Select this option to disable Code ID processing. The barcode data is received, but is not checked for a Code ID.
- **AIM:** Programs an internal scanner to transmit the AIM ID with each barcode. After clicking the Symbology Settings button, the Symbology listing includes all AIM ID symbologies plus any configured custom Code IDs. Select this option to enable processing of barcodes with an AIM or custom Code ID.
- **Symbol:** Programs an internal scanner to transmit the Symbol ID with each barcode. After clicking the Symbology Settings button, the Symbology listing includes all Symbol ID symbologies plus any configured custom Code IDs. Select this option to enable processing of barcodes with a Symbol or custom Code ID. Note that the Symbol entry may not appear for any device equipped with an integrated imager (e.g. EV-15 imager).
- **Custom:** Does not change the internal scanner's Code ID transmission setting. After clicking the Symbology Settings button, the Symbology listing includes all Custom Code IDs. Select this option to enable processing of barcodes with a custom Code ID.

Notes

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the barcode data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e. treated as a Code ID).
- **UPC/EAN Codes only**: The code id for supplemental barcodes is not stripped.
- When Enable Code ID is set to **AIM or Symbol,**Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to **Custom**, Custom Code IDs replace the list of standard Code IDs.
- When Enable Code ID is set to **Custom**, **AIM** or **Symbol** Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 ']A1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID :]A1AAA.
- When Enable Code ID is set to **None**, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- When using the parameters in the Scanner Control Panel to manage indicators for good read/bad read decoding, the number or patterns of beeps heard may be confusing. Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from an external scanner triggers a good scan beep, and then the rejection of scanned barcode data by the Scanner Control Panel processing causes a bad scan beep by the mobile device on the same data.

Barcode – Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for barcodes that do not use the standard AIM or Symbol IDs or for barcodes that have data embedded at the beginning of the data that acts like a Code ID.

These are called **custom Code ID**s and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a barcode, the configuration specified for the custom Code ID is applied to the barcode data.

It is intended that custom code IDs are used to supplement the list of standard code IDs (if **Enable Code ID** is set to **AIM** or **Symbol**), or to replace the list of standard code IDs (if **Enable Code ID** is set to **Custom).**

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*

The dialog box shown below allows the custom Code IDs to be configured. When incoming data is checked for a custom ID code, the list is compared in the order displayed in this dialog box.

After adding, changing and removing items from the Custom IDs list, click the OK button to save changes and return to the Barcode panel.

Parameters

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Click on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is clicked, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button text changes to a Remove button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration Data	Translation	Example Control Character	Example Configuration	Translated Data
Ignore (drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	Ignore (drop)	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	STX	0x02 in a barcode is converted to the text STX.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	^M	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass through to the application.	Horizontal Tab	\^I	Value 0x09 in a barcode is converted to the text ^I.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	0x0A	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass through to the application.	Vertical Tab	\0x0A or 0\x0A	Value 0x0C is a barcode is converted to text 0x0A

See also *Hat Encoding*

Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	**EAN-128(]C1)**	**EAN-13(]E0)**	**Intrlv 2 of 5(]I0)**	**Code93**
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		*123	1*	456	
Strip Trailing	0	0	3	3	
Prefix	aaa	bbb	ccc	ddd	
Suffix	www	xxx	yyy	zzz	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

Barcode Symbology	**Raw Scanner Data**	**Resulting Data**
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	*< rejected > (too short)*
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	***< rejected >*** *(too long)*
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	***< rejected >*** *(disabled)*
Code-93	]G0444444	***< rejected >*** *(disabled)*
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	***< rejected >*** *(too short)*

Note: Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

Barcode - Ctrl Char Mapping

The Ctrl Char Mapping button (Control Character Mapping) activates a dialog to define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values.

In key message mode, control characters can also be translated to their control code equivalent key sequences.

Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

Parameters

Translate All

This option is grayed unless the user has Send Key Messages (WEDGE) on the Main tab selected.

In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent control key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad).

Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke.

Any control code without a keystroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names.

When a character name is selected from the drop down box, the default text *Ignore (drop)* is shown and highlighted in the Replacement edit control. *Ignore (drop)* is highlighted so the user can type a replacement if the control character is not to be ignored.

Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default *Ignore (drop)* in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character.

Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then clicking the button. The assigned replacement is then added to the list box above the Assign button.

For example, if Carriage Return is replaced by Line Feed (by specifying ^J or 0x0A) in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements.

All replacements are enclosed in single quotes to delimit white space that has been assigned.

Assign Button

Click this button when you want to assign the characters in the Replacement text box to the character in the Character drop down box.

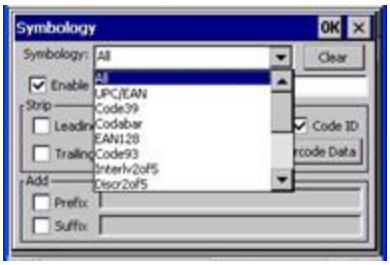
Delete Button

This button is grayed unless an entry in the list box is highlighted.

When an entry (or entries) is highlighted, and the Delete button is clicked, the highlighted material is deleted from the list box.

Barcode - Symbology Settings

The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured. The features available on the Symbology Settings dialog include the ability to individually enable or disable a barcode from scanning, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode.



The Symbology drop-down box contains all symbologies **supported on the HX2**. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.

Clear Button -- Clicking this button will erase any programmed overrides, returning to the default settings for the selected symbology. If **Clear** is pressed when **All** is selected as the symbology, a confirmation dialog appears, then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

*Note: When **Enable Code ID** is set to **None** on the Barcode tab and when **All** is selected in the Symbology field, **Enable** and **Strip Code ID** on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.*

When **All** is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Barcode tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as Code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults.

If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for **All** are used which is not necessarily the default.

Parameters

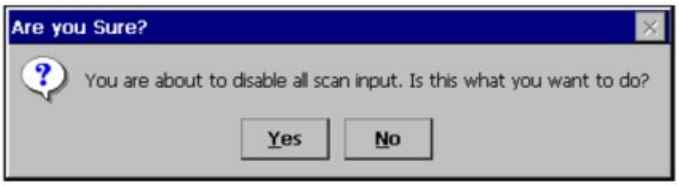
Enable

This checkbox enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the barcode data for the type of ID specified in the Barcode tab -- Enable Code ID field (AIM or Symbol) plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming barcode data, if the symbology is disabled, the barcode is rejected. Otherwise, the other settings in the dialog are applied and the barcode is processed. If the symbology is disabled, all other fields on this dialog are grayed.

When there are ***no*** *customized symbology settings*, and the Enable checkbox is unchecked, while All is selected, a warning message is displayed.



Click the Yes button or the No button. Click the X button to close the dialog without making a decision.

If there ***are*** *customized settings*, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies *except* the customized ones.

Min

This field specifies the minimum length that the barcode data (not including Code ID) must meet to be processed.

Any barcode scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

Max

This field specifies the maximum length that the barcode data (not including Code ID) can be processed. Any barcode scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

This group of controls determines what data is removed from the barcode before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.

If the total number of characters being stripped is greater than the number of characters in the barcode data, it becomes a zero byte data string. If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the barcode data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

This strips the number of characters specified from the end of the barcode data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Code ID

Strips the Code ID based on the type code id specified in the Enable Code ID field in the Barcode tab. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise).

Barcode Data Match List

Barcode Data Panel

This panel is used to strip data that matches the entry in the Match list from the barcode. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.

To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap the OK button to store any additions, deletions or changes.

Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Tap the **Add** button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The **Add** button changes to **Insert**. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The **Add** button changes to **Replace**. When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The **Clear All** button changes to a **Remove** button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length barcode, a good beep will still be sounded, since barcode data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ***ABC*** and ***AB***, in that order, incoming data with ***ABC*** will match first, and the ***AB*** will have no effect.
- When a match between the first characters of the barcode and a string from the list is found, that string is stripped from the barcode data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard ***** is not specified, the string is assumed to strip from the beginning of the barcode data. The string ***ABC**** strips off the prefix ***ABC***. The string ****XYZ*** will strip off the suffix ***XYZ***. The string ***ABC*XYZ*** will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard ***?*** may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The Barcode Data is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of **Strip: Code ID** in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the barcode data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the barcode data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see *Hat Encoding and Decimal-Hexadecimal Chart* sections in the *Appendix* for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

Add Prefix	To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the prefix is added for any symbology that has not been specifically configured.
Add Suffix	To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the suffix is added for any symbology that has not been specifically configured.

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. F1), arrow keys, Page up, Page down, Home, and End.

Length Based Barcode Stripping

Use this procedure to create symbology rules for two barcodes with the same symbology but with different discrete lengths. This procedure is not applicable for barcodes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

- A normal AIM or Symbol symbology role can be created for the desired barcode ID.
- Next, a custom barcode symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

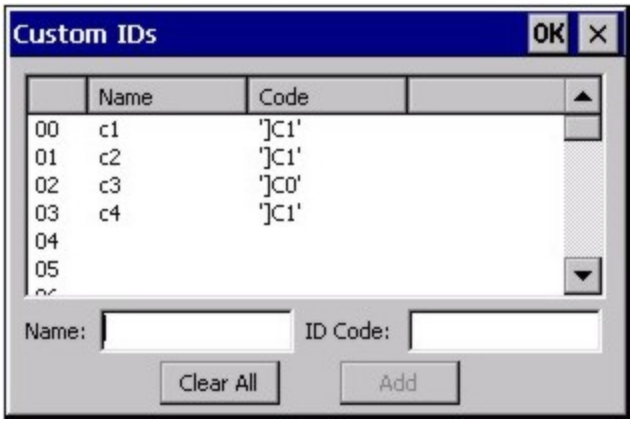
For the purposes of this example, the following sample barcode parameters will be used – EAN 128 and Code 128 barcodes. Some of the barcodes start with '00' and some start with '01'. The barcodes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character barcode is Code 128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

On the Barcode tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN 128 barcode and 0 for Code 128 barcode.

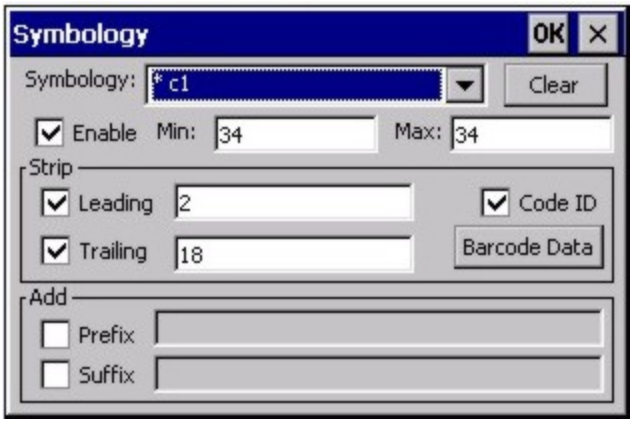
- c1 = Code = ']C1'
- c2 = Code = ']C1'
- c3 = Code = ']C0' (24 character barcode is Code 128)
- c4 = Code = ']C1'



AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"

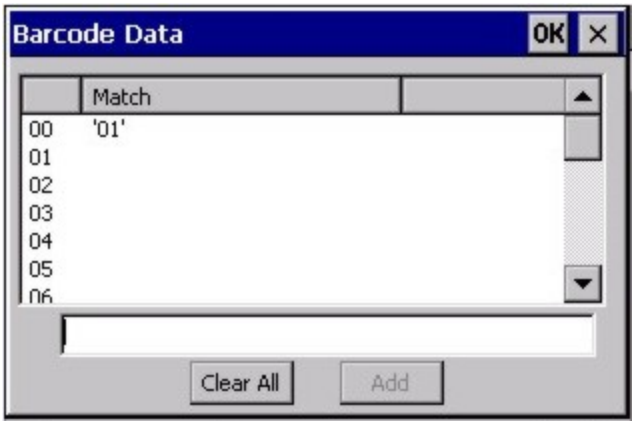
Add the AIM custom symbologies. Refer to the previous section *Barcode – Symbology Settings* for instruction.



Click the Barcode Data button.

Click the Add button.

Add the data for the match codes.



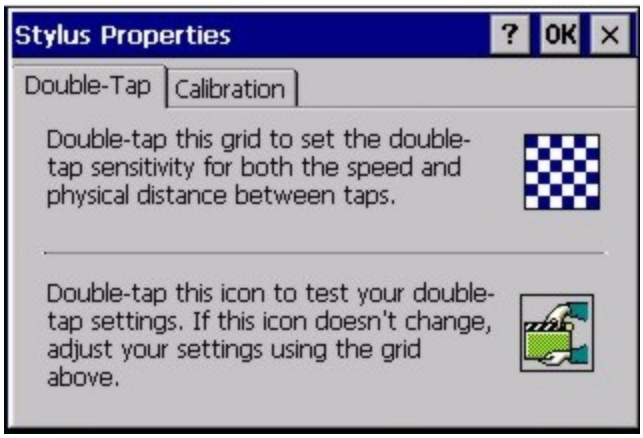
Refer to the previous section Barcode Data Match List for instruction.

Scan a barcode and examine the result.

Stylus

Start | Settings | Control Panel | Stylus

Use this control panel option to set stylus double-tap sensitivity properties and calibrate the HX2 touch panel when needed.



Double Tap

Follow the instructions on the screen and tap the OK button to save any double tap changes.

Calibration Tab

Calibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To begin, tap the **Recalibrate** button on the screen with the stylus. Press and hold the stylus on the center of the target as it moves around the screen. Press the Enter key to keep the new calibration setting or press the Esc key to revert to the previous calibration settings.

System

Start | Settings | Control Panel | System

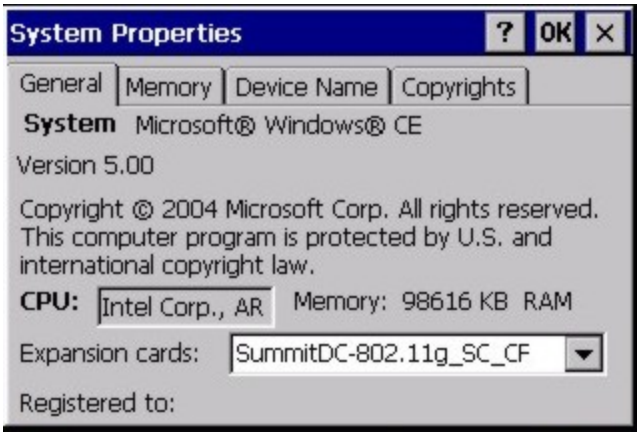
Use these HX2 panels to:

- Review System and mobile device data and revision levels.
- Adjust Storage and Program memory settings.
- Assign a device name and device descriptor.

Factory Default Settings

General	No user interaction
Memory	1/3 storage, 2/3 program memory
Device Name	Unique to equipment type
Device Description	LXE_*unique to equipment type*
Copyrights	No user interaction

General Tab

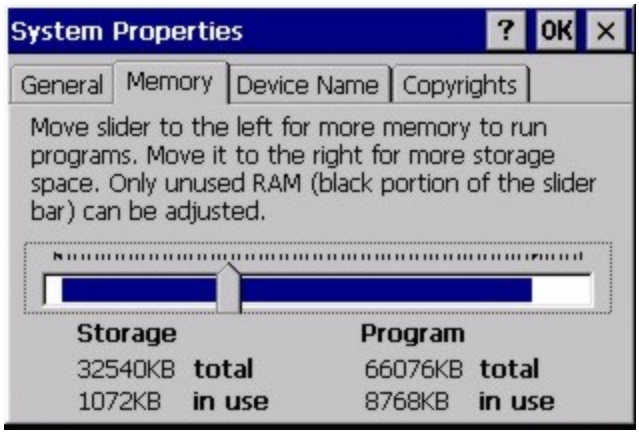


System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

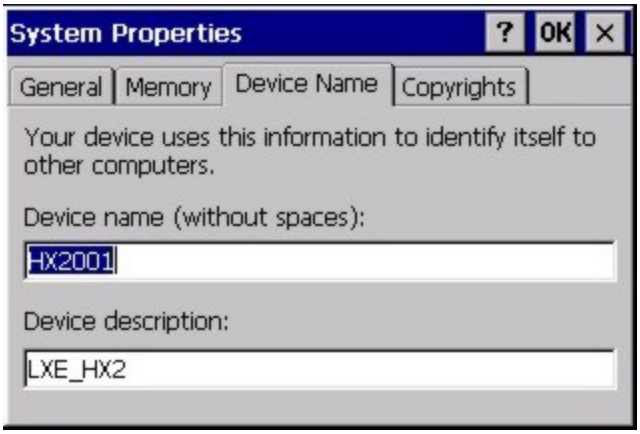
Memory sizes given do not include memory used up by the operating system. For example, a system with 128 MB may only report 99 MB memory, since 29 MB is used by the operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory Tab



Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory.

Device Name Tab



The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. This information is used to identify the HX2 to other computers and devices.

Copyrights Tab

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Volume and Sounds

Start | Settings | Control Panel | Volume & Sounds

Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

Set volume parameters and assign sound WAV files to CE events using these options.

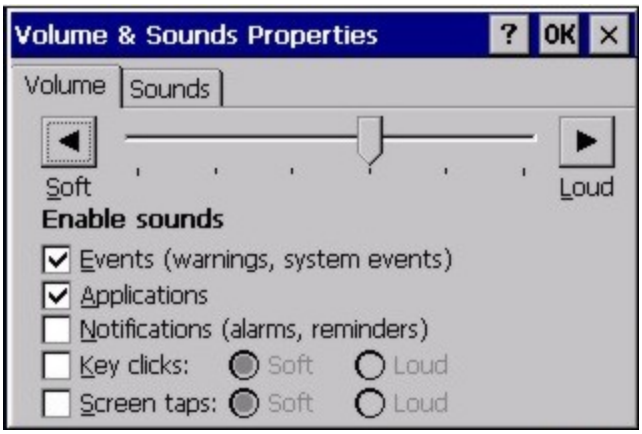
You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

As the volume scrollbar is moved between Loud and Soft, the HX2 emits a tone each time the volume increases or decreases.

Volume must be enabled when you want to adjust volume settings using keypad keys.

Factory Default Settings

Volume	
Events	Enabled
Application	Enabled
Notifications	Disabled
Volume	Middle of Bar
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!



The volume setting is stored in the registry and is recalled at power on.

Note: Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned barcode data by the barcode processing causes a bad scan beep from the mobile device on the same data.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice.

By default a good scan sound on the HX2 is a single beep, and a bad scan sound is a double beep.

WiFi Control Panel

Start | Settings | Control Panel | WiFi or click the Summit Client Utility icon

Use this option to set parameters and manage profiles for the wireless client pre-loaded on your HX2. See the Summit Client Utility for more information.

Enabler Installation and Configuration

Introduction

This section discusses LXE supported features with Wavelink Avalanche Mobile Device Servers. This section is split into three basic areas:

- Installation
- User Interface
- Enabler Configuration

Installation

To use the Wavelink Avalanche MC System, the following items are required:

- A desktop or laptop PC on which to install the Avalanche MC Console.
- A desktop or laptop PC on which to install the Avalanche Mobile Device Server (this can be the same PC where the Avalanche MC Console is installed).
- Wavelink Avalanche MC Console 4.2 or later.
- A Wavelink Device License for each client device.

To use Avalanche Remote Control, the follow additional items are required:

- Wavelink Remote Control plug-in, 2.0 or later
- A Wavelink Remote Control License for each client device

Installing the Enabler on LXE Devices

LXE CE devices have the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped from LXE. The installation files are located in the \System folder on CE devices.

*Note: **Important:** If the user is NOT using Wavelink Avalanche to manage their mobile device(s), the Enabler should not be installed on the mobile device(s). Doing so results in unnecessary delays when booting the device.*

Briefly . . .

The Avalanche Enabler installation file LXE_ENABLER.CAB is loaded on the HX2 by LXE; however, the device is not configured to launch the Enabler installation file automatically. The installation application must be run manually the first time Avalanche is used.

Note: Older versions of the Enabler may have a device specific name such as LXE_XXX_ENABLER.CAB.

After the installation application is manually run, the Enabler will, by default, be an auto-launch application.

This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

The RMU.CE.CAB (Remote Management Utility) file is placed on the device during manufacturing in the \System\RMU folder.

During the Enabler installation process, the Enabler checks for the RMU.CE.CAB file in the \System folder.

- If present, it assumes the RMU.CE.CAB file is already installed and continues.
- If the file RMU.CE.CAB file is not present, it looks for the file in the \System\RMU folder.
- If present, the Enabler copies the file to the \System folder and installs it.

At this point, the OS will automatically install the RMU after the HX2 reboots.

Enabler Uninstall Process

To remove the LXE Avalanche Enabler from the HX2:

- Delete the Avalanche folder located in the \System directory.
- Warm boot the HX2.

The Avalanche folder cannot be deleted while the Enabler is running. See Stop the Enabler Service.

If sharing errors occur while attempting to delete the Avalanche folder, warm boot the HX2, immediately delete the Avalanche folder, and then perform another warm boot.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Mobility Center Console:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the HX2 desktop.
2. Select **File | Settings**.
3. Select the **Startup/Shutdown** tab.
4. Select the **Do not monitor or launch Enabler** parameter to prevent automatic monitoring upon startup.
5. Select **Stop Monitoring** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.
6. Click the **OK** button to save the changes.
7. **Reboot** the HX2 if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on the HX2 can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server PC and the HX2.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server PC and the HX2.
- Wirelessly via the HX2 2.4GHz radio and an access point

After installing the Enabler on the HX2 the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network.

The Enabler running on the HX2 will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the LXE barcode wedge panels on the HX2).

The wireless connection is made using the default wireless [radio] interface on the mobile device therefore the HX2 must be actively communicating with the network for this method to succeed.

If a Mobile Device Server is found, the Enabler automatically attempts to apply all wireless and network settings from the active profile. The Enabler also automatically downloads and processes all available packages.

If the Enabler does not automatically detect the Mobile Device Server, the IP address of the Mobile Device Server can be entered on the Connect tab of the Enabler setup. Please see Enabler Configuration for details.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the HX2 Enabler attempts to apply all network and wireless settings contained in the active profile.

The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler.

These local parameters cannot be overridden from the Avalanche MC Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled for Windows CE devices

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the **Enabler icon** on the desktop.
2. Select **File | Settings**.
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for **Manage Network Settings**, **Manage Wireless Settings** and **Use Avalanche Network Profile**.
6. Click the **OK button** to save the changes.
7. **Reboot** the device.

Preparing an LXE Device for Remote Management

Two additional utilities are necessary for remote management.

- The **LXE Remote Management Utility (RMU)** must be installed on all LXE mobile devices first – then you can control mobile device reboot, storage RAM adjustment, real-time updates and Avalanche Enabler properties. If the RMU is not already installed on the HX2, see Using Wavelink Avalanche to Upgrade System Baseline.
  If in doubt, verify RMU.CE.CAB exists in the \System folder. If the RMU.CE.CAB file is present when the Enabler is installed, the RMU is also installed.

  Important: If the OS package includes double-byte Asian fonts, the storage RAM property of the RMU must be higher than the default value (40MB).

  If the amount of storage RAM is too low, the Enabler returns a "Mobile unit out of resources" error.

  To determine the minimum value required, inspect the RMU.StorageRAM>=*nn* parameter in the Criteria field for the OS package. Generally, this setting should be approximately 40 MB above the amount of RAM in use on the device for a standard OS and 50MB above the amount of RAM in use for an OS with Asian fonts.

  For example, if after installing all the software, the device shows 5MB in use, this setting should be about 45MB for a standard OS, 55 MB for an Asian font OS.
- Use the LXE **Wireless Configuration Application (WCA)** when you want to remotely manage the Summit client device. This utility is downloaded and installed in addition to the LXE Remote Management Utility. The WCA is included when the Summit radio driver software is updated. The WCA is automatically installed when the radio driver is updated.

If the LXE Remote Management Utility (RMU) is not present on the HX2, see Using Wavelink Avalanche to Upgrade System Baseline.

Using Wavelink Avalanche to Upgrade System Baseline

This procedure assumes the Avalanche Enabler is already installed on the HX2 and is already in communication with the Avalanche MC Console.

Part 1 – Bootstrapping the RMU

1. Install the RMUCEbt package into the Avalanche MC Console. Do NOT include the Reboot option as part of the configuration (i.e. the **Reboot button** in the "Reboot Options" branch must be unbolded).
2. Enable ONLY the RMUCEbt package in the Avalanche MC Console and update the devices. The RMU is downloaded and automatically installed.
3. **Disable** the RMUCEbt package in the Avalanche MC Console.
4. For each device, **double-click** on the device to open the Client Controls dialog box.
5. Check the **Delete Orphaned Packages** checkbox and click the **Update Now** button.
6. After the sync completes, uncheck **Delete Orphaned Packages** and close the dialog box.

Part 2 – Installing Packages

1. **Enable** the RMUCE package in the Avalanche MC Console.
2. **Enable** all remaining packages and send them down. It is important that you include the new OS package in this group (be sure to include the Enabler). If the radio is to be managed remotely, it is important to include the radio package in this group so that after the reboot the radio can automatically associate. If the radio package is not sent, the device loses connection to the network and manual configuration of the radio parameters is required.
3. Set the Reboot setting for the OS package to **Auto**.
4. After all packages are downloaded (this may take several minutes) the Remote Management Utility (RMU) is launched. The RMU processes all the downloaded packages. If the radio package was downloaded, the Wireless Configuration Application (WCA) is launched to process the new radio settings.
5. After the RMU finishes installing all the packages, the device is automatically coldbooted (assuming the Reboot setting was set to Auto in Step 3).
6. After the Device completes the coldboot, the RMU is autoinstalled by the OS and the previously downloaded packages are restored. Assuming at least one package has registry settings that were restored, and that package was set to reboot (either auto or prompt), the RMU then performs an automatic warmboot.
7. After the warmboot, the device is configured.
8. If the device will no longer be monitored by Wavelink Avalanche, you may remove the Enabler to eliminate boot up delays, if desired. Even if the Enabler is removed, the installed packages and their configurations continue to be restored with every reboot by the RMU.

Version Information on LXE Mobile Devices

The VersionInfo.EXE file is included in the Remote Management Utility package downloaded to the HX2. It is stored in the \Program Files\RMU folder. When VersionInfo.EXE is opened, a dialog box is presented to the HX2 user displaying:

- Remote Management Utility (RMU) version
- Wireless Configuration Application (WCA) version

VersionInfo displays the version for each utility only after that utility has been executed at least once.

User Interface

The Enabler can be configured and controlled manually through the user interface on the HX2. This section details the functionality that can be controlled by the user or system administrator.

Parameters and Screen Displays

Screen displays shown in this section are designed to present the end-user with information graphically.

Placement of information on the screen displays may be split between one or many tabbed panels.

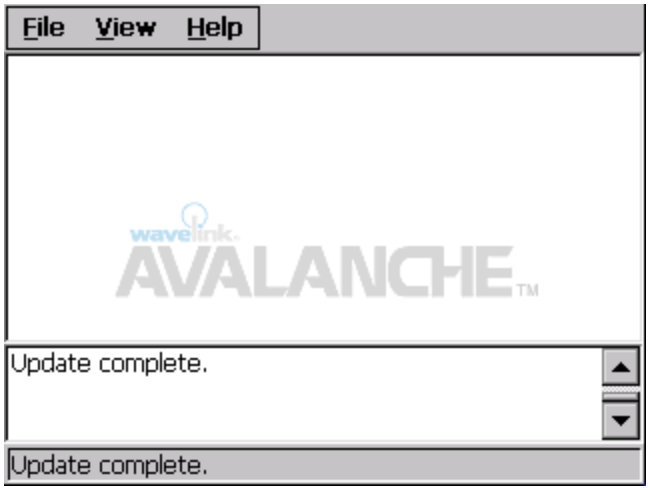
Standard Avalanche Enabler parameters that are not supported by LXE may be missing or dimmed (visible but unable to be edited) on the tabbed panels or screen displays.

Enabler Configuration

 Enabler Settings Icon

The Enabler user interface application is launched by clicking either the **Enabler Settings icon** on the desktop or Taskbar or by selecting **Avalanche Enabler** from the Programs menu.

The opening screen presents the HX2 user with the connection status and a navigation menu.



Avalanche Enabler Opening Screen

Note: Some parameters and features described in this section may not be available if you are not running the latest version of the Enabler. Contact your LXE representative for upgrades.

File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the HX2 immediately upon a successful connection.
Scan Config	*Note: LXE does not support the Scan Configuration feature.* The Scan Config option under the File menu allows the user to configure Enabler settings using a special barcode that can be created using the Avalanche MC Console utilities. Refer to the Wavelink Avalanche Mobility Center User Guide for details.
Settings	The Settings option under the File menu allows the HX2 user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected.  The default Settings password is **system** The password is not case-sensitive.

Avalanche Update using File | Settings

Use these menu options to setup the Avalanche Enabler on the HX2. LXE recommends changing settings and then saving the changes (reboot) before connecting to the network.

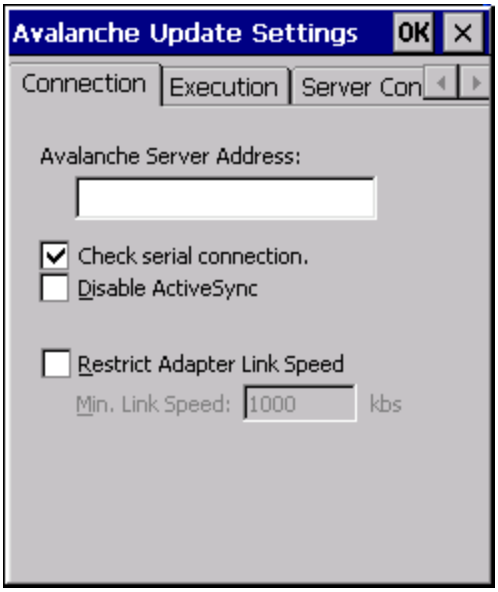
Alternatively, the Mobile Device Server can be disabled until needed (refer to the **Wavelink Avalanche Mobility Center User's Guide** for details).

Menu Options

Note: Your HX2 screen display may not be exactly as shown in the following menu options. Contact your LXE representative for version information and upgrade availability.

Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF connections are used to check for the presence of the Mobile Device Server.
Execution	*Not available in this release*. LXE recommends using AppLock, which is resident on each Windows CE device.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Startup/Shutdown	Set options for Enabler program startup or shutdown.
Taskbar	Set options for Taskbar.
Scan Config	This option allows the user to configure Enabler settings using a special barcode that is created by the Avalanche MC Console. *Scan Config not currently supported by LXE.*
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

Connection



Connection Options

Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the HX2.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable ActiveSync	Disable ActiveSync connection with the Mobile Device Server.
Restrict Adapter Link Speed	Default is disabled. Minimum Link Speed dimmed.

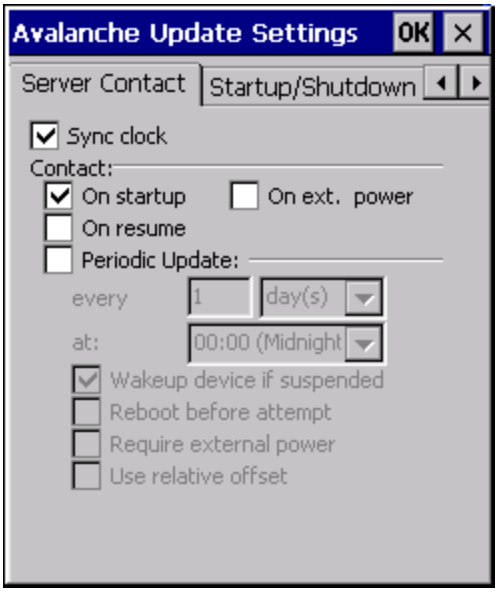
Execution

Note the dimmed options on this HX2 panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.

Execution Options (Dimmed)

Auto-Execute Selection	An application that has been installed with the Avalanche Management system can be run automatically following each boot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Management System.
Delay before execution	Time delay before launching Auto-Execute application.

Server Contact



Server Contact Options

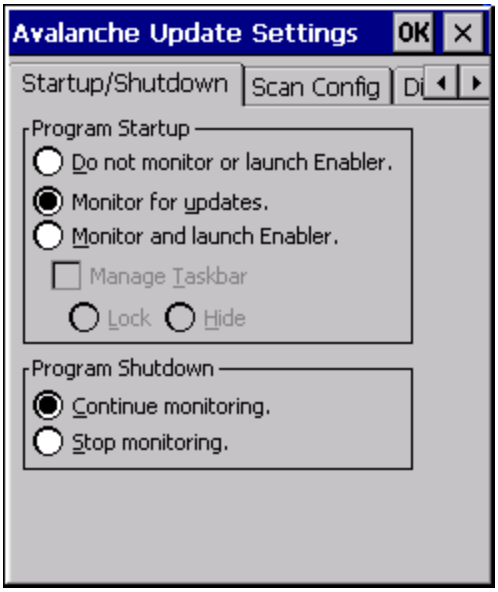
Note: Your HX2 screen display may not be exactly as shown above. Contact your LXE representative for upgrade availability and version information.

Sync Clock	Reset the time on the HX2 based on the time on the Mobile Device Server host PC.
Contact	On Startup – Connect to the Mobile Device Server when the Enabler is accessed.
	On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.
	On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as based on a docking event.
Periodic Update	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can wakeup and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.
Require external power	Only connect when the mobile device has external power.
Use relative offset	Dimmed.

Startup/Shutdown

LXE recommends using LXE AppLock to manage the taskbar. AppLock is resident on each mobile device with a Windows CE OS (with the exception of the HX3). AppLock configuration instructions are located in the HX2 reference guide.

If the Startup/Shutdown tab is not present on the Enabler installed on your device, please see the equivalent options on the Preferences tab and the Taskbar tab.



Startup / Shutdown Options

Do not monitor or launch Enabler	When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
Monitor for updates	Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
Monitor and launch Enabler	Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Manage Taskbar (Lock or Hide)	Note the dimmed options. The Enabler can restrict user access to other applications when the user interface is accessed by either locking or hiding the taskbar.
Program Shutdown (Continue or Stop monitoring)	The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited.

Preferences

LXE recommends using LXE AppLock to manage the taskbar. AppLock is resident on each mobile device with a Windows CE OS.

If the Preferences tab is not present on the Enabler installed on your device, please see the equivalent options on the Startup/Shutdown tab.

Preferences Options

Administration

By default, *Keep settings unlocked for 10 minutes* is disabled (checkbox is blank).

Application

Default value - Monitor for Updates

The following options are available for startup and shutdown monitoring:

- Do not Monitor - When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server. (Startup only).
- Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
- Launch User Interface - Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application. (Startup only).
- Exit Application - The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited. (Shutdown only).

Activity Log

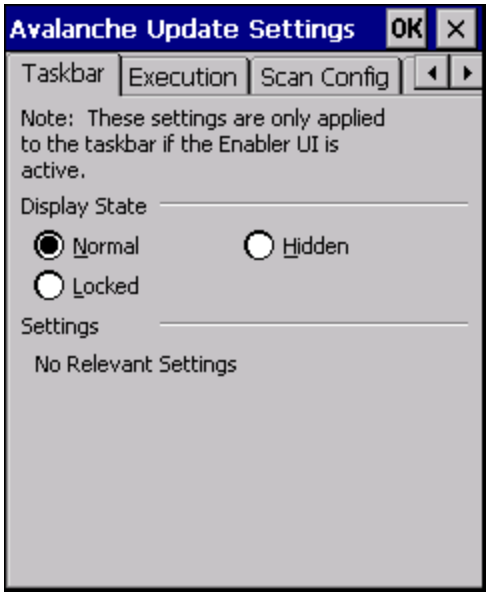
Default value - No Activity Log

Use this option to control the level of log kept while Enabler is running.

Taskbar

LXE recommends using LXE AppLock to manage the taskbar. AppLock is resident on each mobile device with a Windows CE OS (with the exception of the HX3). AppLock configuration instructions are located in the HX2 reference guide.

If the Taskbar tab is not present on the Enabler installed on your device, please see the equivalent options on the Startup/Shutdown tab.



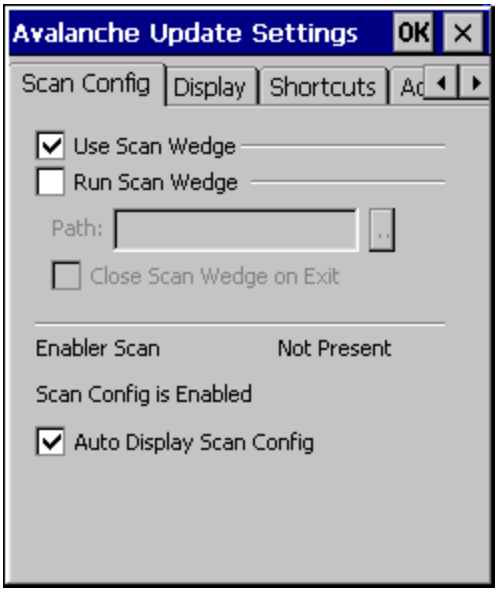
Taskbar Options

The Display State options control the appearance of the taskbar while using the Enabler interface.

- Normal - taskbar is visible, taskbar icons function normally.
- Hidden - taskbar is not displayed
- Locked - taskbar is visible, but most icons are hidden or for information only.

Scan Config

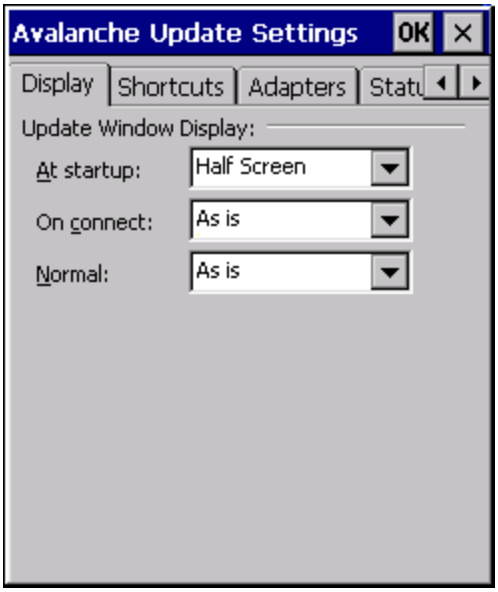
LXE recommends using *LXE eXpress Config* and *eXpress Scan* for this function. eXpress Scan is included with the updated HX2 enablers.



Scan Config Option

Scan Config functionality is a standard option of the Wavelink Avalanche MC system but is *not currently supported by LXE* on the HX2.

Display



Window Display Options

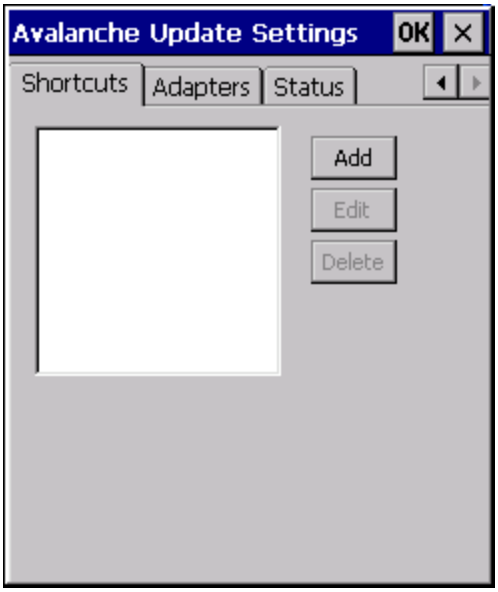
Update Window Display

The user interface for the Enabler can be configured to dynamically change based on the status of the HX2 connection with the Mobile Device Server.

At startup	Default is Half Screen. Options are Half screen, Hidden or Full screen.
On connect	Default is As Is. Options are As is, Half screen, or Full screen.
Normal	Default is As Is. Options are Half screen, Hidden or As Is.

Shortcuts

LXE recommends using *LXE AppLock* for this function. AppLock is resident on each mobile device with a Windows CE OS.



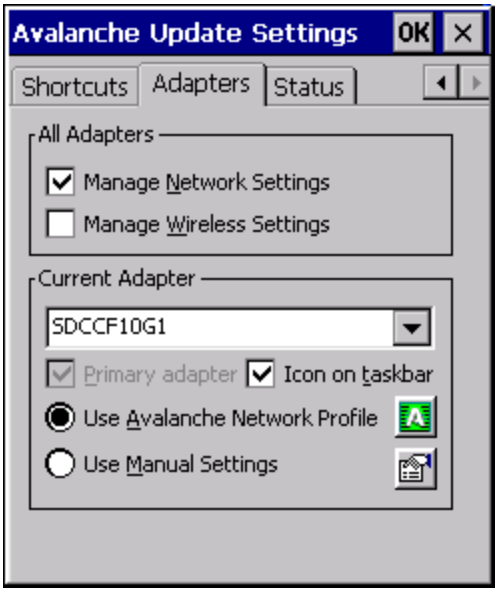
Application Shortcuts

Configure shortcuts to other applications on the HX2. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

LXE recommends using *LXE AppLock* for this function.

Adapters

Note: LXE recommends the user review the network settings configuration utilities and the default values before setting All Adapters to Enable in the Adapters applet.



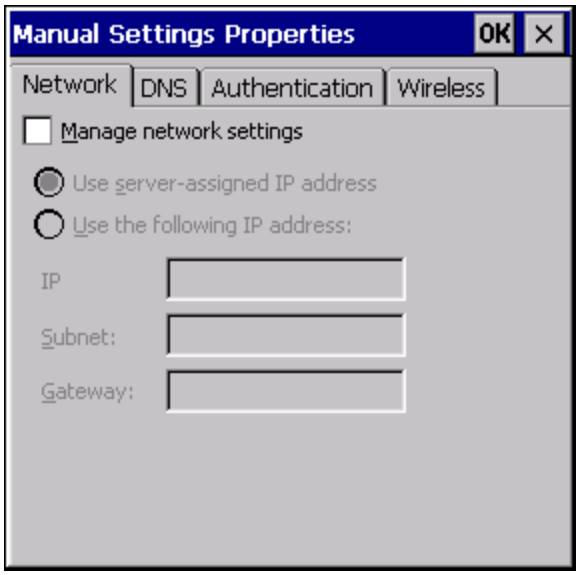
Adapters Options - Network

Manage Network Settings	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. For Summit clients, Manage Wireless Settings should not be checked as LXE's configuration packages provide more radio configuration options.
Current Adapter	Lists all network adapters currently installed on the HX2.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.
Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Mobile Device Server.

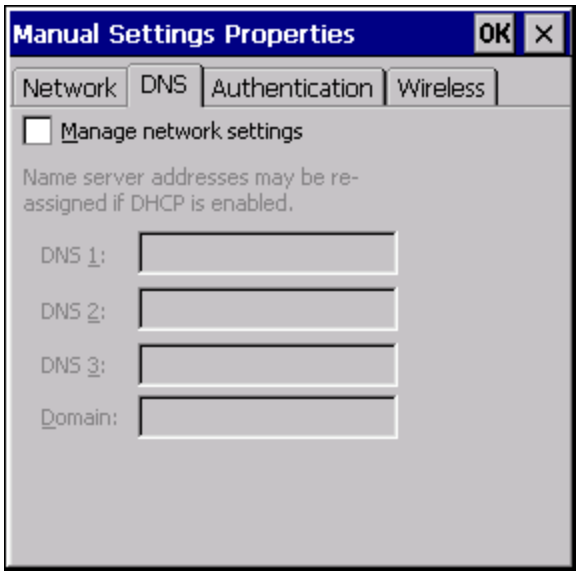
Avalanche Icon 	Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.  **Avalanche Network Profile Displayed**
Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche MC Console and use only the network settings on the HX2.
Properties Icon	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.

Network

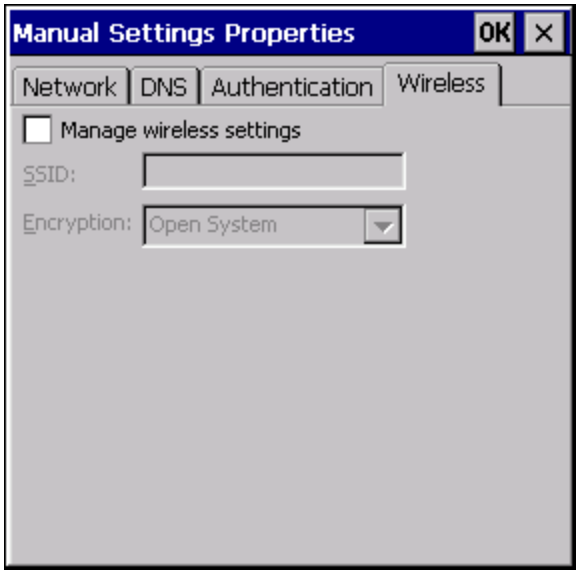


DNS



Authentication

Wireless



Manual Settings Properties Panels

Note: The Authentication tab may not be present in all versions of the Enabler.

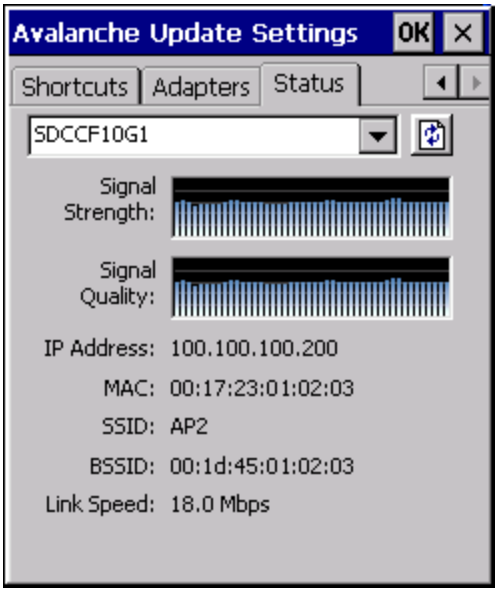
LXE does not recommend enabling “Manage Wireless Settings” for Summit Client devices.

Troubleshooting: When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global Manage wireless settings and Manage network settings options are enabled on the Adapters panel (see Figure titled Adapters Options – Network, earlier in this section). Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the HX2 network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button.

When the Windows Refresh button is tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.



Status Display

Link speed indicates the speed at which the signal is being sent from the adapter to the HX2. Speed is dependent on signal strength.

Exit

The Exit option is password protected. The default password is **leave**. The password is not case-sensitive.

Exit Password

If changes were made on the HX2 Startup/Shutdown tab screen, then after entering the password, tap OK and the following screen is displayed:

Continue or Stop Monitoring

Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Using Remote Management

1. Configure the radio to connect to the network running the Mobile Device Server. After the HX2 is connected, proceed to step 2.
2. If it is desired to configure the radio using the Summit package, add the configured package to the Wavelink Avalanche MC Console and enable it.
3. Verify RMU.CE.CAB exists in the \System\RMU folder.
4. Double click the HX2 enabler CAB file in the \System folder.
5. The enabler automatically launches after installation and contacts the Mobile Device Server. The Avalanche MC Console connected to that Mobile Device Server identifies the remote device and performs a sync. This downloads any available packages available for the HX2.

Using eXpress Scan

eXpress Scan Desktop Icon

If the HX2 has an eXpress Scan icon on the desktop, eXpress Scan may be used for the initial configuration of the device.

If the eXpress Scan icon is not present on the desktop, install the Enabler. If the icon is still not present, the Enabler must be updated.

If the eXpress Scan icon is present, follow these steps to configure the HX2 to connect with the wireless network and the Mobile Device Server.

Step 1: Create Barcodes

Barcodes are created with the eXpress Config utility on the desktop/laptop computer, not the mobile device. Depending on the barcode length and the number of parameters selected, eXpress Config generates one or more barcodes for device configuration. The barcodes contain configuration parameters for the wireless client in the LXE device and may also specify the address of the Mobile Device Server.

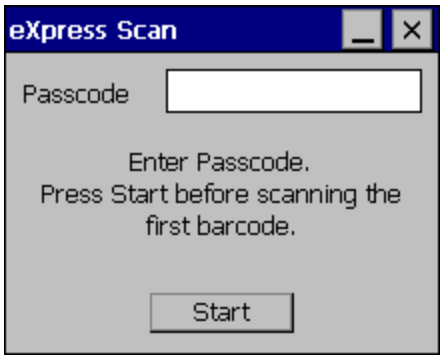
Barcodes should be printed at a minimum of 600 dpi.

Step 2: Scan Barcodes

For each LXE device to be configured, please follow these instructions.

Start eXpress Scan on the HX2 by double clicking the eXpress Scan icon.

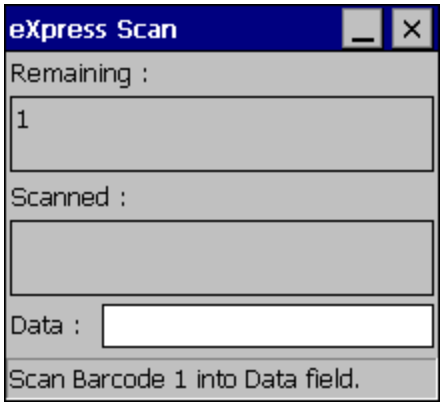
Enter the barcode password, if any.



eXpress Scan Password Input

Click Start.

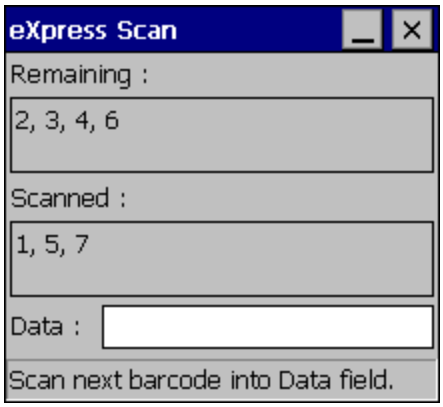
Barcode 1 must be scanned first. The scanned data is displayed in the “Data” text box. The password, if any, entered above is compared to the password entered when the barcodes were created.



Scan Barcode 1

If the passwords match, the barcode data is processed and the screen is updated to reflect the number of barcodes included in the set.

If the passwords do not match, an error message is displayed. The current screen can be closed using the X box in the upper right corner. The password can be re-entered and Barcode 1 scanned again.



Scan Remaining Barcodes

The remaining barcodes may be scanned in any order. After a barcode is scanned, that barcode is removed from the "Remaining:" list and placed in the "Scanned:" list.

Step 3: Process Completion

After the last barcode is scanned, the settings are automatically applied.

Configuring Settings

Once configured, the HX2 is warmbooted. Once connected to the wireless network and the Mobile Device Server, any software updates and additional configuration data are downloaded.

Wireless Network Configuration for LXE Devices

The Summit client device is either an 802.11g radio, capable of both 802.11b and 802.11g data rates or an 802.11a radio, capable of 802.11a, 802.11b and 802.11g data rates.The radio can be configured for no encryption, WEP encryption or WPA security.

Security Options Supported are

- None
- WEP
- LEAP
- WPA-PSK
- WPA/LEAP
- PEAP-MSCHAP
- PEAP-GTC
- EAP-TLS
- EAP-FAST

Important Notes

	It is important that all dates are correct on the HX2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail. Verify and adjust the date using the Date and Time control panel.
	It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact your LXE representative for details.
	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, warmboot the HX2.

Summit Client Utility

Note: When making changes to profile or global parameters, the device should be warmbooted afterwards.

Access:

Start | Programs | Summit | SCU *or*

SCU Icon on Desktop *or*

Summit Tray Icon (if present) *or*

Wi-FI Icon in the Windows Control Panel (if present)

The Main Tab provides information, admin login and active profile selection.

Profile specific parameters are found on the Profile Tab. The parameters on this tab can be set to unique values for each profile. This tab was labeled Config in early versions of the SCU.

The Status Tab contains information on the current connection.

The Diags Tab provides utilities to troubleshoot the radio.

Global parameters are found on the Global Tab. The values for these parameters apply to all profiles. This tab was labeled Global Settings in early versions of the SCU.

Help

Help is available by clicking the ? icon in the title bar on most SCU screens.

The SCU help may also be accessed by selecting Start | Help and tapping the Summit Client Utility link. The SCU does not have to be accessed to view the help information using this option.

Summit Tray Icon

 The Summit tray icon provides access to the SCU and is a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Click the icon to launch the SCU.

Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Wireless Zero Config Utility and the Summit Radio

- The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.
- You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. LXE recommends using the Summit Client Utility to connect to your network. The Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

How To: Use the Wireless Zero Config Utility

1. Select **ThirdPartyConfig** in the Active Profile drop down list as the active profile (see Main Tab).
2. Warmboot the device.

The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings. There may be a slight delay before the Wireless Zero Config icon indicates the status of the connection.

How to: Switch Control to SCU

1. To switch back to SCU control, select any other profile in the SCU Active Config drop down list, except **Third-PartyConfig**.
2. Warmboot the device.

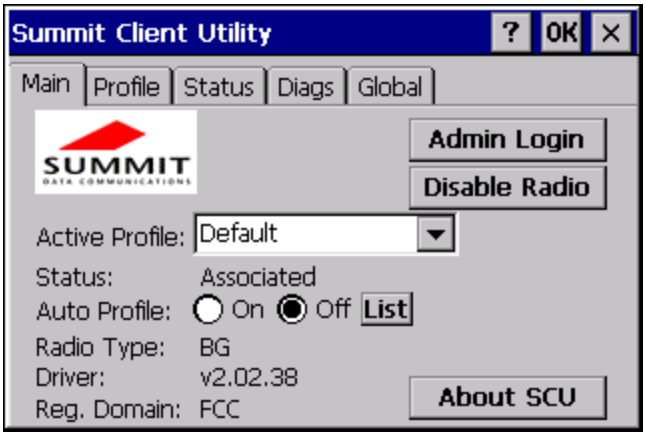
Radio control is passed to the SCU.

Main Tab

Start | Programs | Summit | Main tab

Factory Default Settings

Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC or ETSI



SCU - Main Tab

The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (BG is an 802.11 b/g radio, ABG is an 802.11 a/b/g radio).
- Regulatory Domain
- Copyright Information can be accessed by tapping the About SCU button
- Active Config profile / Active Profile name
- Status of the client (Down, Associated, Authenticated, etc).

The **Active Profile** can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. LXE recommends performing a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named “ThirdPartyConfig” is chosen as the active profile, the Summit Client Utility passes control to Windows Zero Config for configuration of all client and security settings for the network module.

The **Disable Radio** button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

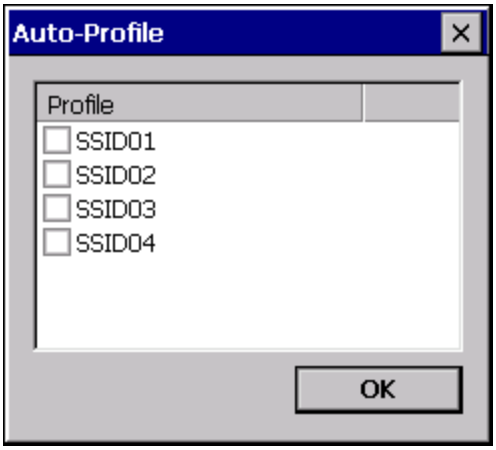
The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the **Admin Logout** button or exit the SCU without tapping the **Admin Logout** button.

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, click the **List** button.



Select Profiles for Auto Profile

The Auto Profile selection screen displays all currently configured profiles. Click on the checkbox for any profiles that are to be included in Auto Profile selection then click ok to save.

To enable Auto Profile, click the **On** button on the **Main** tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is clicked to turn off Auto Profile.

Note: Do not include any profiles with an Ad Hoc Radio Mode in this listing.

Admin Login

To login to Administrator mode, tap the **Admin Login** button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the **Admin Logout** button, or the **OK** button to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.

Main Tab – Enter Admin Password

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap **OK**. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Global tab.

The end-user can:

- Turn the radio on or off on the Main tab.
- Select an active Profile on the Main tab.
- View the current parameter settings for the profiles on the Profile tab.
- View the global parameter settings on the Global tab.
- View the current connection details on the Status tab.
- View radio status, software versions and regulatory domain on the Main tab.
- Access additional troubleshooting features on the Diags tab.

After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the Profile tab.
- Edit global parameters on the Global tab.
- Enable/disable the Summit tray icon in the taskbar.

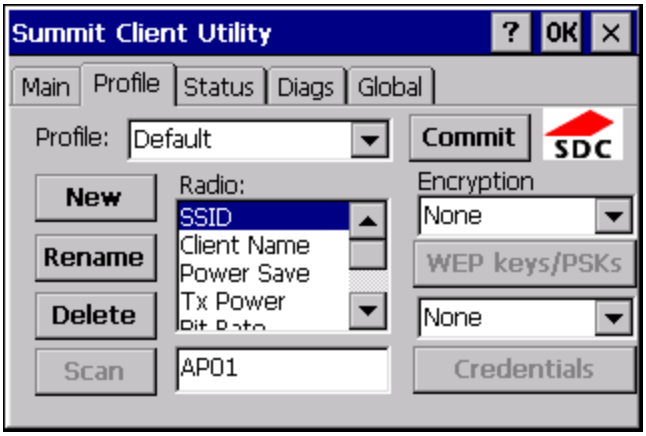
Profile Tab

Start | Programs | Summit | Profile tab

Note: Tap the Commit button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!

Factory Default Settings

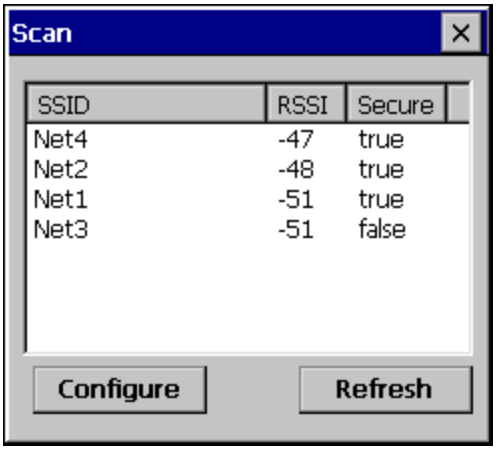
Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See Profile Parameters for default
Auth Type	Open
EAP Type	None
Encryption	None



SCU – ProfileTab

When logged in as an Admin (see Admin Login), use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The Profile tab was previously labeled Config.

Buttons

Button	Function
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
Scan	Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers. If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.  **SCU – Scan** If you are logged in as an Admin, tap an SSID in the list and tap the Configure button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already).
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.

Note: Unsaved Changes – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.

Important – The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

Profile Parameters

Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	Fast	Power save mode is On. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode).
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, PEAP-TLS, EAP-TTLS, or EAP-TLS. *Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.*
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP (or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the HX2. *Note: The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.*

Parameter	Default	Explanation
Radio Mode	BG radio: BG Rates Full Or A radio: BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio (802.11b/g or 802.11a/b/g) installed in the mobile device. Options: B rates only (1, 2, 5.5 and 11 Mbps) BG Rates Full (All B and G rates) G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps) A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) ABG Rates Full (All A rates and all B and G rates with A rates preferred) BGA Rates Full (All B and G rates and all A rates with B and G rates preferred) Ad Hoc (when connecting to another client device instead of an AP) Default: BG Rates Full (for 802.11b/g radios) BGA Rates Full (for 802.11a/b/g radio) *Note: BG radio only – Previous SCU versions may have the default set as BG Rates Full. Depending on the SCU version, either BG Optimized or BG subset is the default.*

It is important the **Radio Mode** parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the HX2 may only connect to APs set for G rates and not those set for B and G rates.

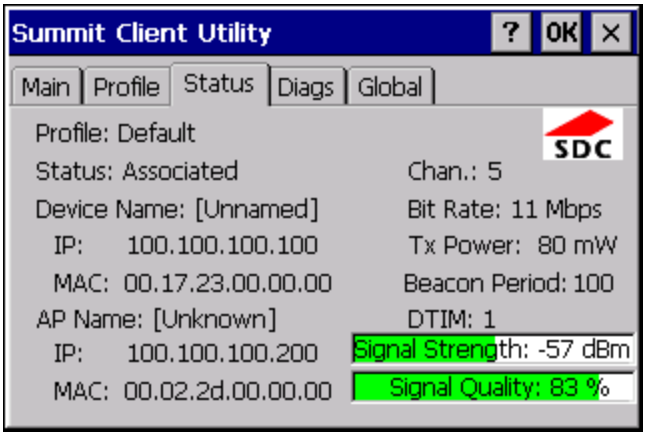
The options for the Radio Mode parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	Radio Mode
A Main and BG Main	ABG Rates Full BGA Rates Full
A Main and A Aux	A Rates Only
BG Main and BG Aux	B Rates Only G Rates Only BG Rates Full BG Subset

Contact your LXE representative if you have questions about the antenna(s) installed on your HX2.

Status Tab

Start | Programs | Summit | Status tab



SCU – Status Tab

This screen provides information on the radio:

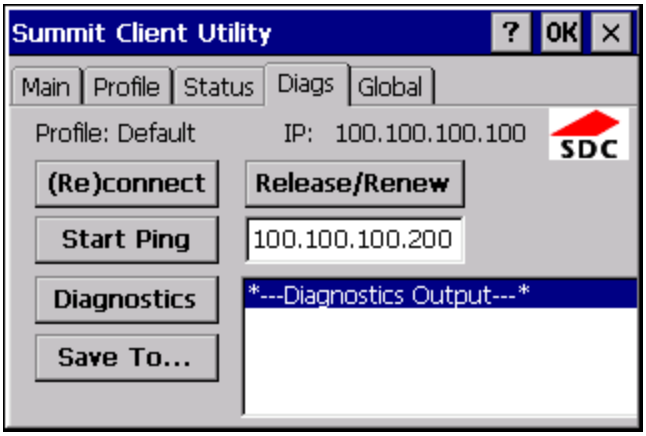
- The profile being used
- The status of the radio card (down, associated, authenticated, etc.)
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic
- Bit rate in Mbit.
- Current transmit power in mW
- Beacon period – the time between AP beacons in kilomicroseconds. (one kilomicrosecond = 1,024 microseconds)
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab

Start | Programs | Summit | Diags tab



SCU – Diags Tab

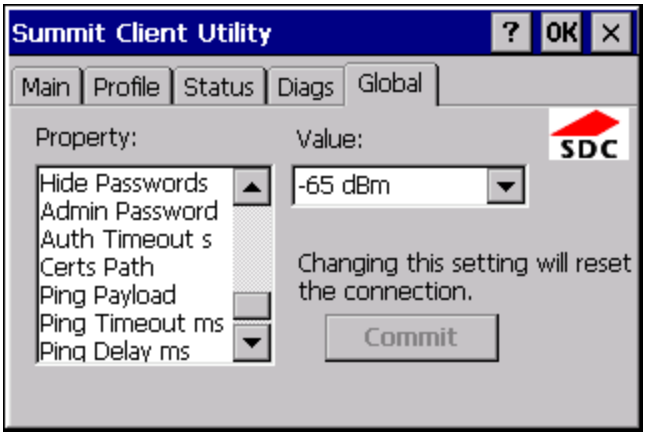
The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to **Stop Ping**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To…** – Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

Start | Programs | Summit | Global tab

The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.



SCU – Global Tab

Note: Tap the Commit button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!

Factory Default Settings	
Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	BG: 10 sec. A: 5 sec.
BG Channel Set	Full
DFS Channels	Off
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	BG: Off A: Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	BG: On A: Main Only
RX Diversity	BG: On-Start on Main A: Main Only
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Passwords	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	System
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms

Custom Parameter Option

LXE does not support the parameter Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

Global Parameters

Parameter	Default	Function
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom. *Note: Available options may vary by SCU revision.*
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.
Roam Period	BG: 10 sec. A: 5 sec.	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
BG Channel Set	Full	Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search, roaming time may be reduced over scanning all channels. Options are: Full (all channels) 1,6,11 (the most commonly used channels) 1,7,13 (for ETSI and TELEC radios only) Custom.
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. *Note: Not supported (always off) in some releases.*
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: 1 through 14 (the 2.4GHz channels) 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX Features	BG: Off A: Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as "On" in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management.

Parameter	Default	Function
		Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off *Note: This parameter cannot be changed for some Summit radios.*
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method), MSCHAPV2, MSCHAP, PAP, CHAP, EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK *Note: This change does not take effect until after a Suspend/Resume cycle.*
WAPI	Off	Default is Off and dimmed (cannot be changed).
TX Diversity	BG: On A: Main Only	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).

The options for the TX Diversity parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	TX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On
BG Main and BG Aux	On

Contact your LXE representative if you have questions about the antenna(s) installed on your HX2.

Parameter	Default	Function
RX Diversity	BG: On-Start on Main A: Main Only	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).

The options for the RX Diversity parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	RX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On-start on Main
BG Main and BG Aux	On-start on Main

Contact your LXE representative if you have questions about the antenna(s) installed on your HX2.

Parameter	Default	Function
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT (or Blank)	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Auth Timeout	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail. If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed. If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials. Options are: An integer from 3 to 60.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certifcates store. LXE suggests ensuring the Windows folder path currently exists before assigning the path in this parameter. See Certificates for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out. Options are: none. For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.

Parameter	Default	Function
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.

Note: Tap the Commit button to save changes. If this panel is closed before tapping the Commit button, changes are not saved!

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers these choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

How to: Use Stored Credentials

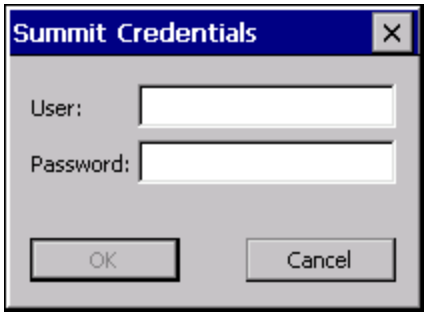
1. After completing the other entries in the profile, click on the **Credentials** button.
2. Enter the Username and Password on the Credentials screen and click **the OK** button.
3. Click the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password..
11. Click the **OK** button then the **Commit** button.
12. If changes are made to the stored credentials, click **Commit** to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Note: See Configuring the Profile for more details.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

How to: Use Sign On Screen

1. After completing the other entries in the profile, click on the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
3. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the **Validate serve**r and **Use MS store** checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
7. Click the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Click the **OK** button.



Sign-On Screen

10. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status Tab indicates the device is Authenticated and the method used.
11. The sign-on screen is displayed after a reboot.

Note: See Configuring the Profile for more details.

If a user enters invalid credentials and clicks **OK**, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user clicks the **Cancel** button, the device does not associate. The user is not prompted again for credentials until:

- the device is rebooted,
- the radio is disabled then enabled,
- the **Reconnect** button on the Diags Tab is clicked or
- the profile is modified and the **Commit** button is clicked.

Windows Certificate Store vs. Certs Path

Note: It is important that all dates are correct on the HX2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see Generating a User Certificate.
- To import the user certificate into the Windows certificate store, see Installing a User Certificate.
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use the Certs Path

1. See Generating a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Please note the location chosen for certificate storage should persist after a reboot.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the CA Cert textbox.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use Windows Certificate Store

1. See Generating a Root CA Certificate and follow the instructions to download the Root Certifcate to a PC.
2. To import the certificate into the Windows store, See Installing a Root CA Certificate.
3. When completing the Credentials screen for the desired authentication, be sure to check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate click on the **Browse (…)** button.

Choose Certificate

6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and click the **Select** button to return the selected certificate to the CA Cert textbox.
8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Configuring the Profile

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

- On the Main Tab, click the Admin Login button and enter the password.
- LXE recommends editing the default profile with the parameters for your network. Select the Default profile from the pull down menu.
- Make any desired parameter changes as described in the applicable following section determined by network security type and click the **Commit** button to save the changes.

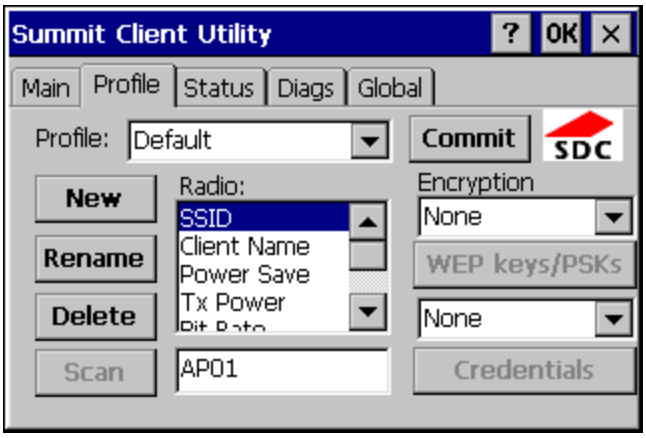
IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the *stored credentials*, click Commit to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **None**
- Set **Auth Type** to **Open**



No Security Profile Configuration

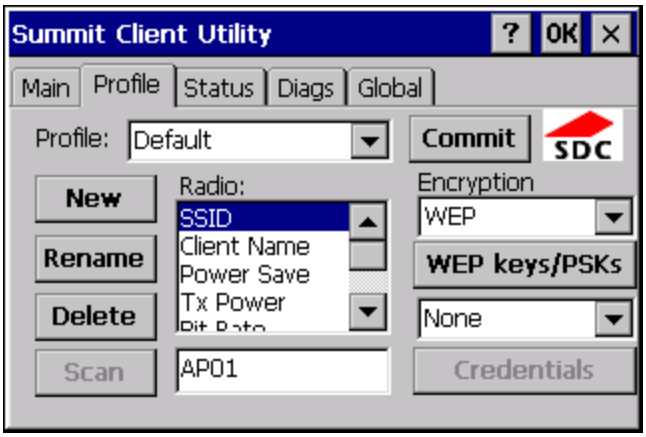
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

WEP

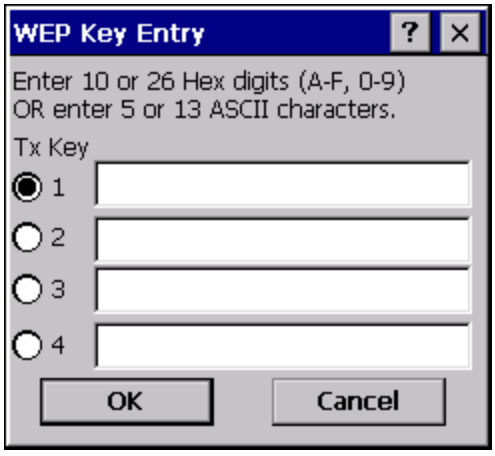
To connect using WEP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WEP** or **Manual WEP** (depending on SCU version)
- Set **Auth Type** to **Open**



WEP Profile Configuration

Click the **WEP keys/PSKs** button.



WEP Keys

Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and click **OK**.

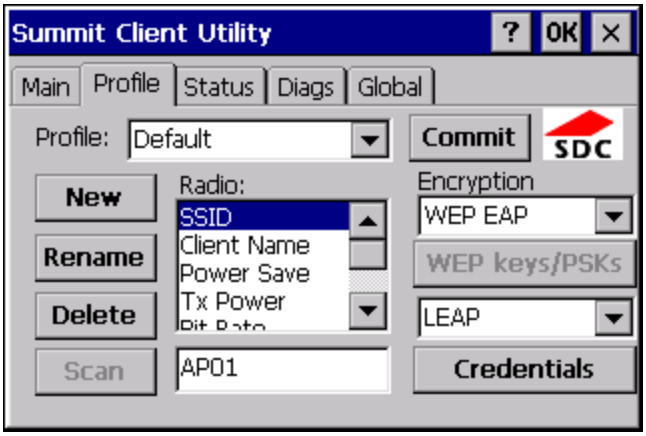
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

To use LEAP (without WPA), make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WEP EAP** or **Auto WEP** (depending on SCU version)
- Set **Auth Type** as follows:
    - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
    - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
    - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.



LEAP Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.

LEAP Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

Click **OK** then click the **Commit** button.

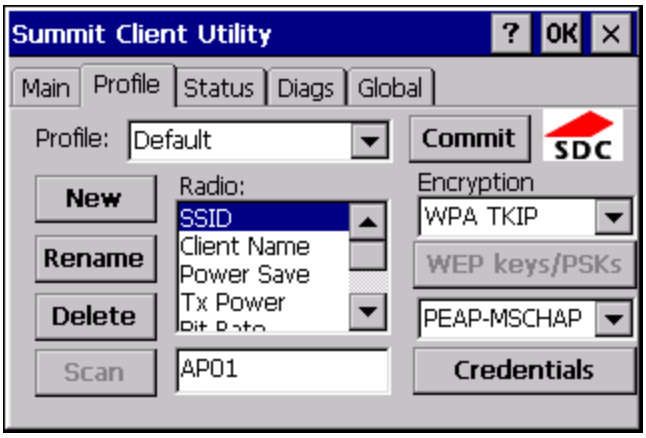
Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-MSCHAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



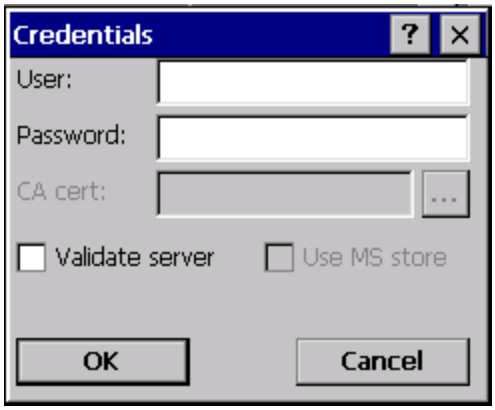
PEAP/MSCHAP Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



PEAP/MSCHAP Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

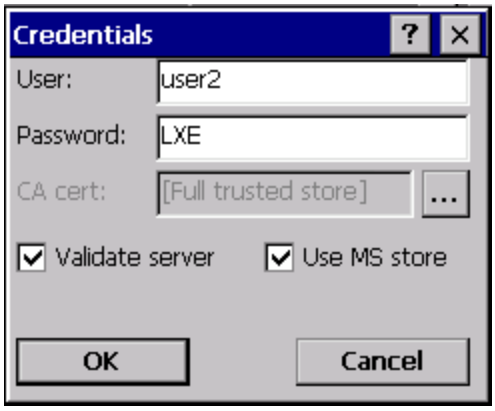
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active profile is selected on the Main Tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



PEAP/MSCHAP Certificate Filename

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store** box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

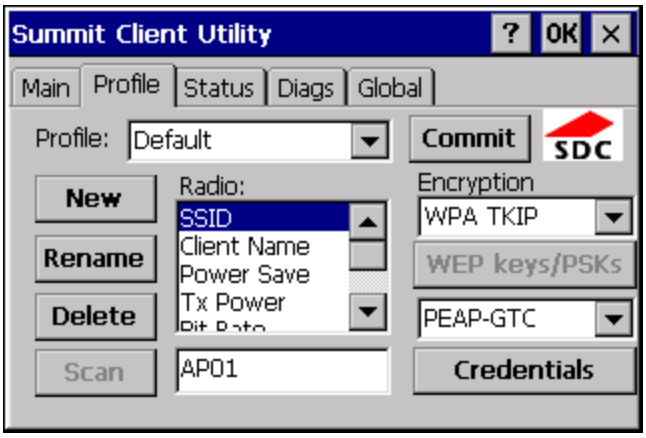
Note: The date must be properly set on the device to authenticate a certificate.

PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-GTC**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



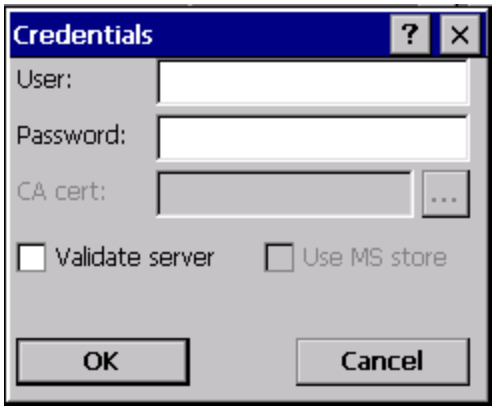
PEAP/GTC Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.

Enter these items as directed below.



PEAP/GTC Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

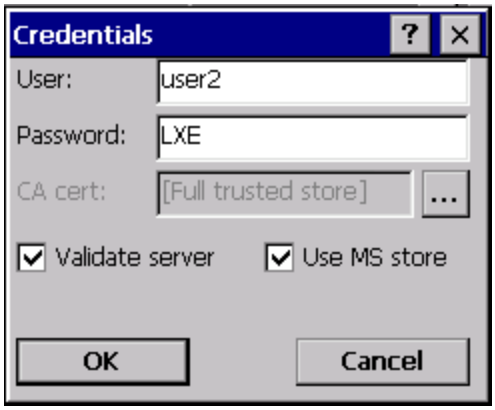
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main Tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



PEAP/GTC Certificate Filename

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store box** unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

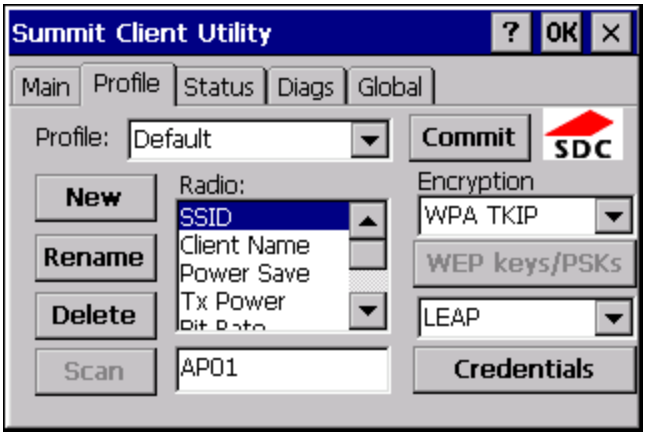
Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** as follows:
    - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
    - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
    - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



WPA/LEAP Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.

WPA/LEAP Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

Click **OK** then click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

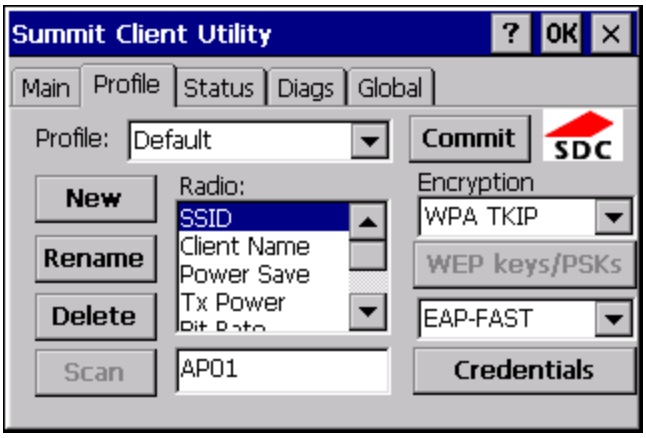
EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-FAST**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the HX2.



EAP-FAST Profile Configuration

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the HX2. The same username/password must be used to authenticate each time. See the note below for more details.

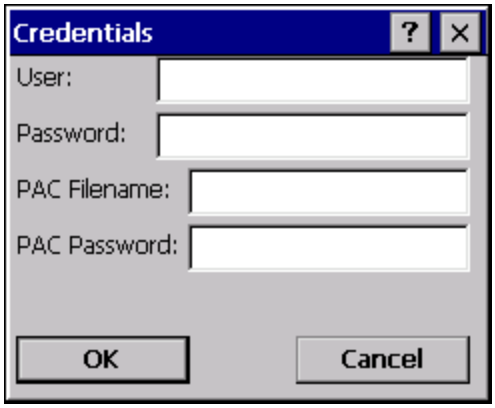
For manual PAC provisioning, the PAC filename and Password must be entered.

See Sign-On vs. Stored Credentials for information on entering credentials.

The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).

Click on the **Credentials** button.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.



EAP-FAST Credentials

To use Sign-On credentials:

- Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.

To use Stored Credentials:

- Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
- Enter the password.

To use Automatic PAC Provisioning:

- No additional entries are required.

To use manual PAC Provisioning:

- Enter the PAC Filename and PAC Password.
- The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.

Tap **OK** then click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

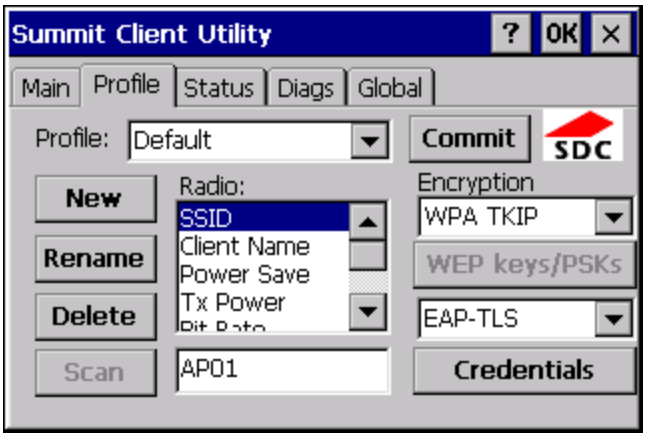
Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System folder with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-TLS**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



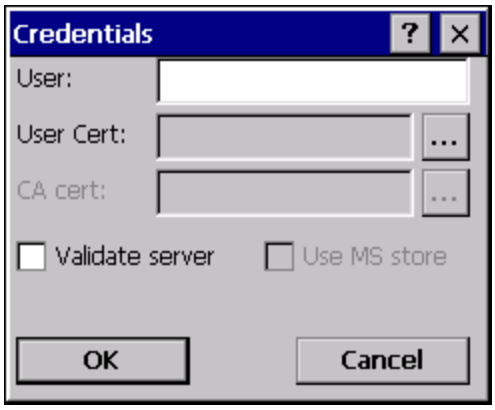
EAP-TLS Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



EAP-TLS Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Leave the certificate file name entries blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main tab.

Once successfully authenticated, import the user certificate into the Windows certificate store.

Return to the Credentials screen.

Use the **Browse** button to locate the User Cert from the certificate store. Highlight the desired certificate and press the **Select** button. The name of the certificate is displayed in the User Cert box.

Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Check the **Validate server** checkbox.

EAP-TLS Credentials

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The HX2 should be authenticating the server certificate and using EAP-TLS for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

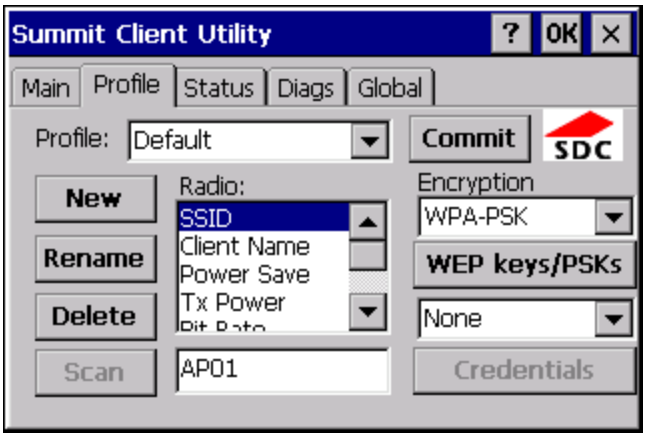
See Certificates for information on generating a Root CA certificate or a User certificate.

Note: The date must be properly set on the device to authenticate a certificate.

WPA PSK

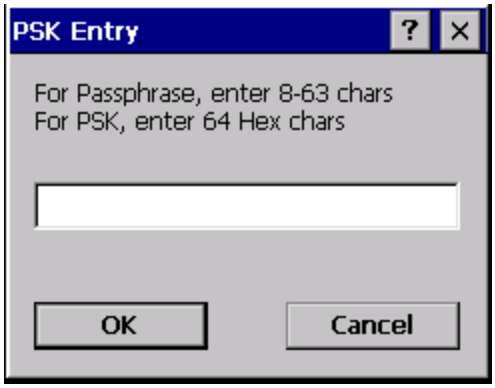
To connect using WPA/PSK, make sure the following profile options are used:

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WPA PSK** or **WPA2 PSK**
- Set **Auth Type** to **Open**



WPA/PSK Profile Configuration

Click the **WEP keys/PSKs** button.



PSK Entry

This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.

Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Note: Please refer to the LXE Security Primer to prepare the Authentication Server and Access Point for communication.

Note: It is important that all dates are correct on the HX2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Quick Start

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. Generate a Root CA Certificate and download it to a PC.
2. Connect the HX2 to the desktop PC using ActiveSync and copy the certificate to the HX2 \System folder.
3. Install the Root CA Certificate.

User Certificates are necessary for EAP-TLS

1. Generate a User Certificate and Private Key file and download it to a PC.
2. Connect the HX2 to the desktop PC using ActiveSync and copy the certificate and private key file to the HX2 \System folder.
3. Install the User Certificate and Private Key file.
4. After installation, perform a Suspend/Resume.
5. Verify installation.

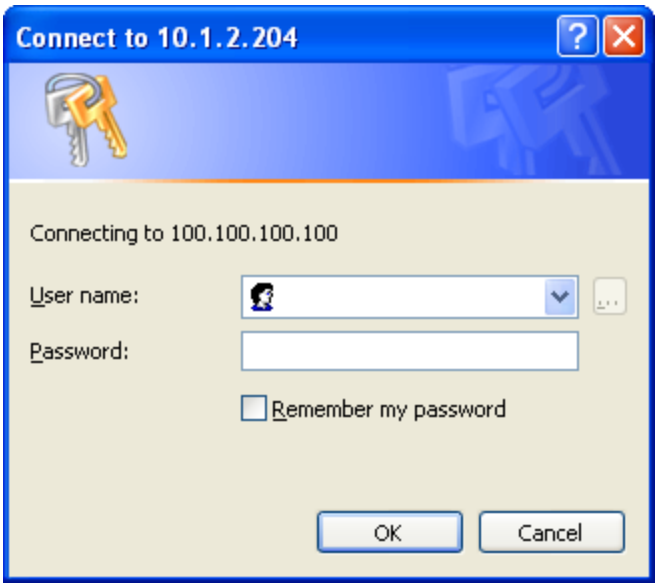
Generating a Root CA Certificate

Note: It is important that all dates are correct on the HX2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

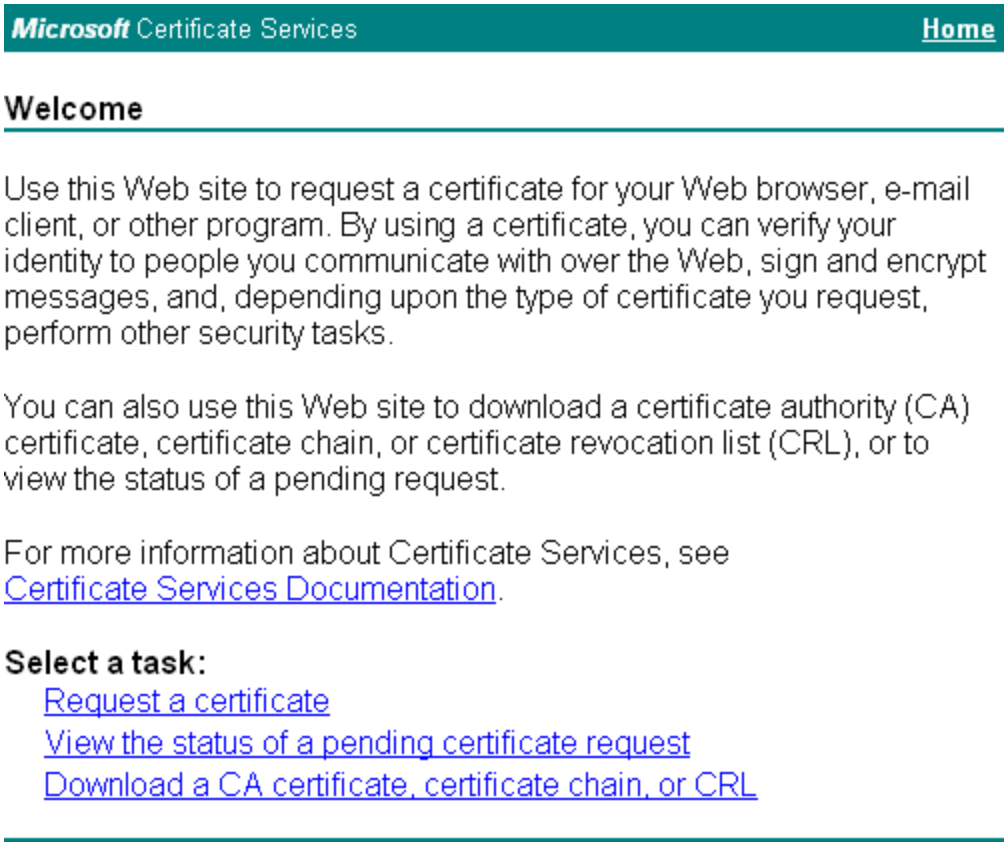
The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the Certificate Authority. To request the root CA certificate, open a browser to

http://<CA IP address>/certsrv.

Sign into the CA with any valid username and password.



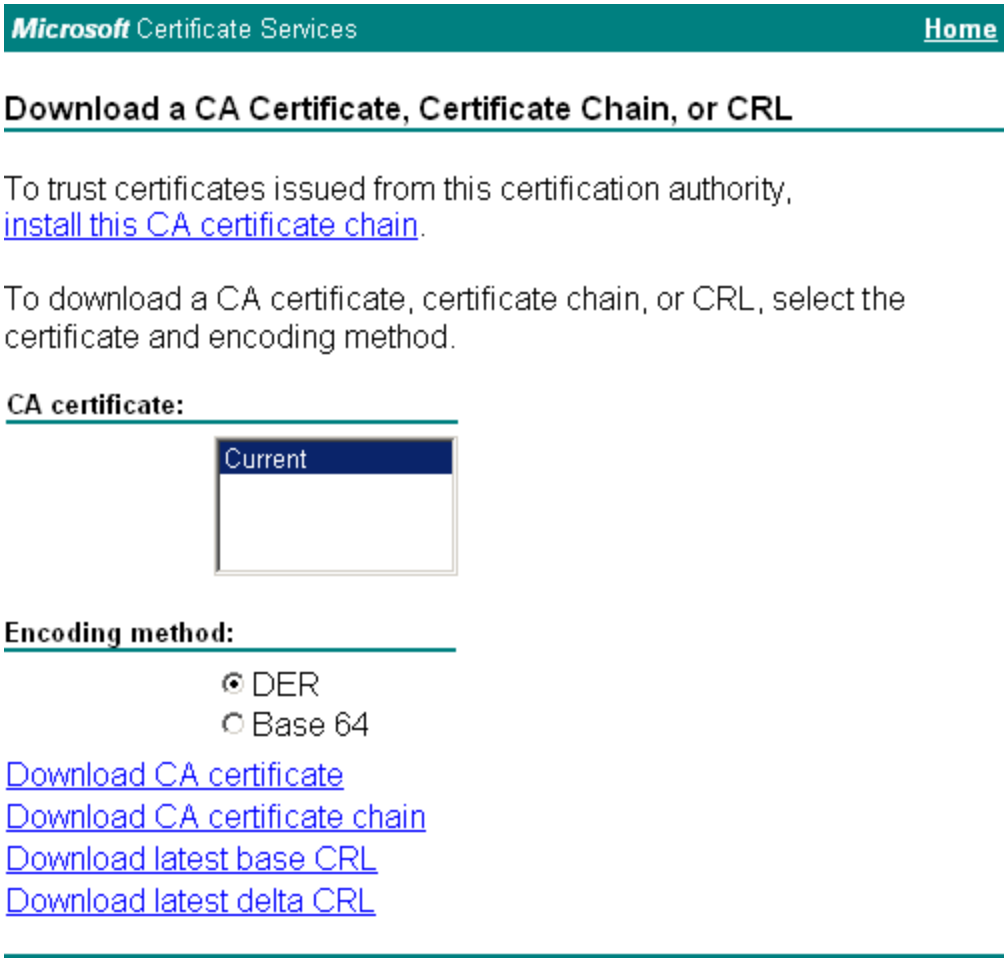
Logon to Certificate Authority



Certificate Services Welcome Screen

Click the **Download a CA certificate, certificate chain or CRL** link.

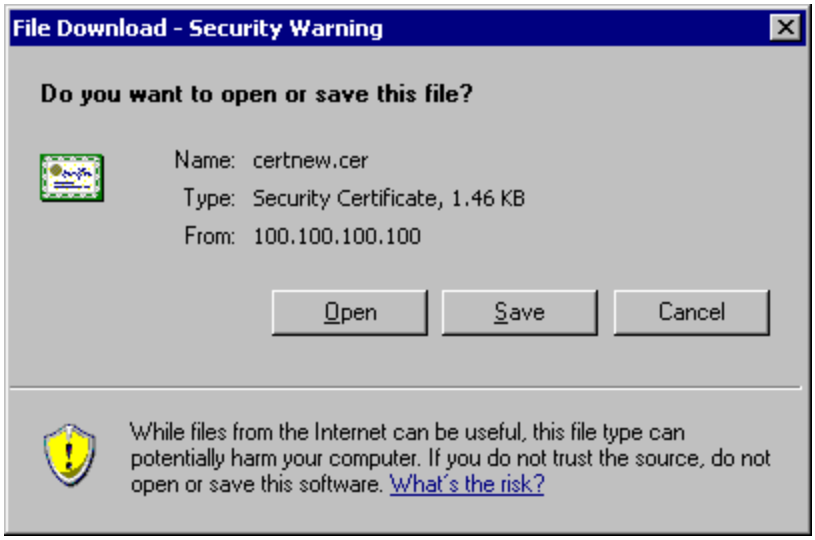
Make sure the correct root CA certificate is selected in the list box.



Download CA Certificate Screen

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.



Download CA Certificate Screen

Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate.

Install the certificate on the HX2.

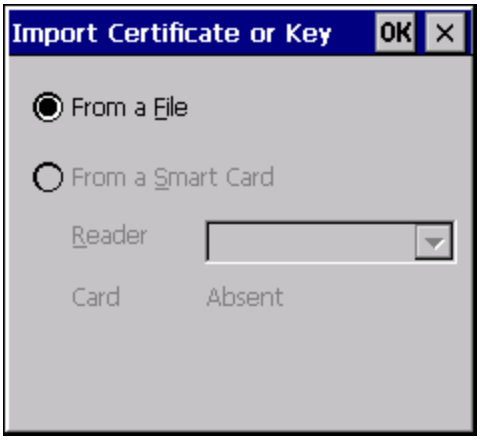
Installing a Root CA Certificate

Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

Copy the certificate file to the HX2. Import the certificate by navigating to **Start | Control Panel | Certificates**.

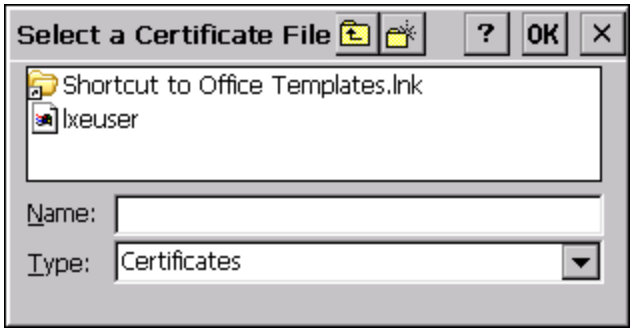
Certificates

Tap the **Import** button.



Import Certificate

Make sure **From a File** is selected and tap **OK**.



Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.

Certificate Import Confirmation

Tap **Yes** to import the certificate.

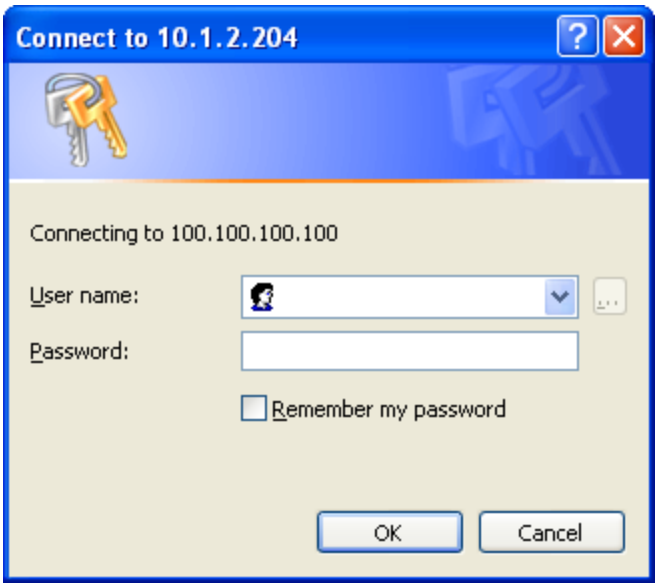
Once the certificate is installed, return to the proper authentication section, earlier in this manual.

Generating a User Certificate

The easiest way to get the user certificate is to use a browser on a PC to navigate to the Certificate Authority. To request the user certificate, open a browser to

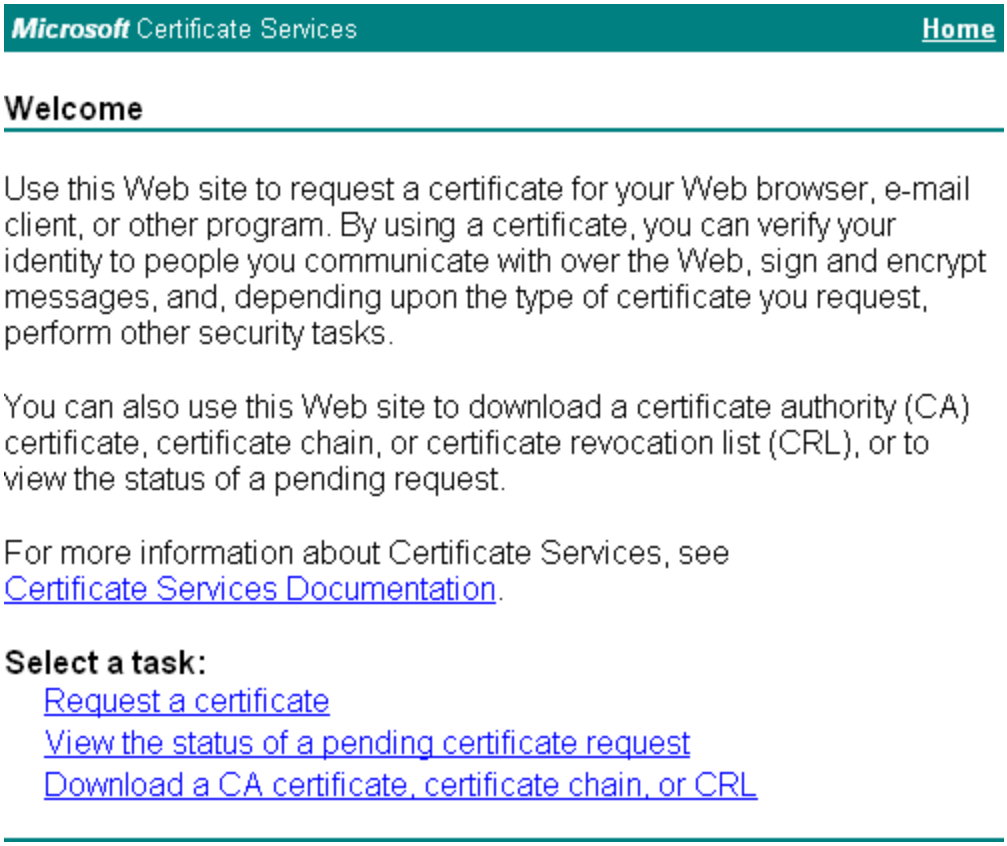
http://<CA IP address>/certsrv.

Sign into the CA with the username and password of the person who will be logging into the mobile device.



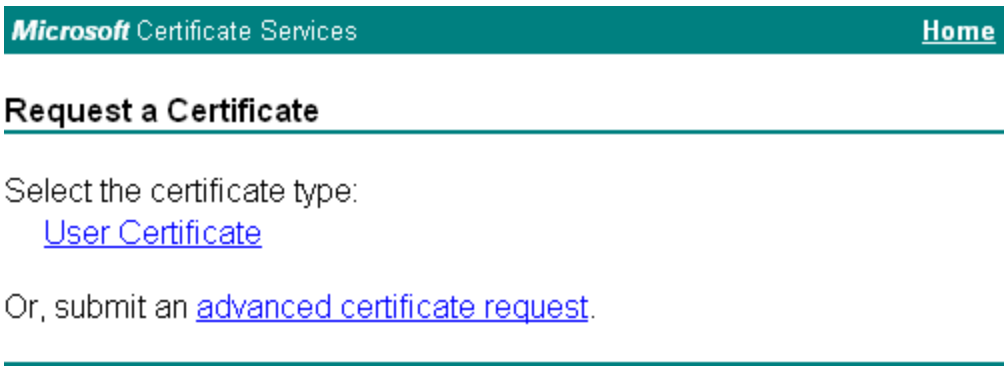
Logon to Certificate Authority

This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the HX2 require the private key to be saved as a separate file rather than including the private key in the user certificate.



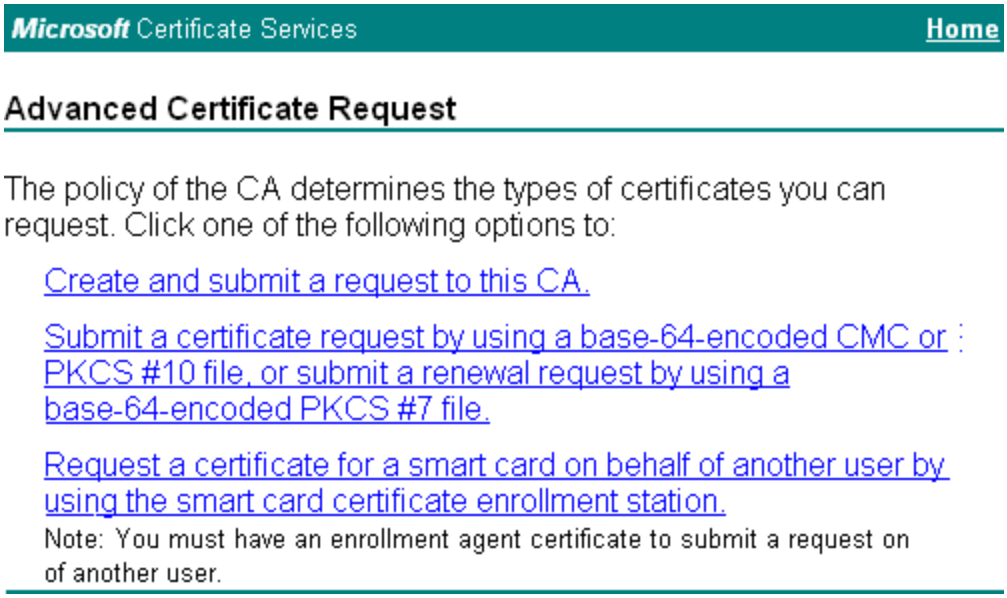
Certificate Services Welcome Screen

Click the **Request a certificate** link.



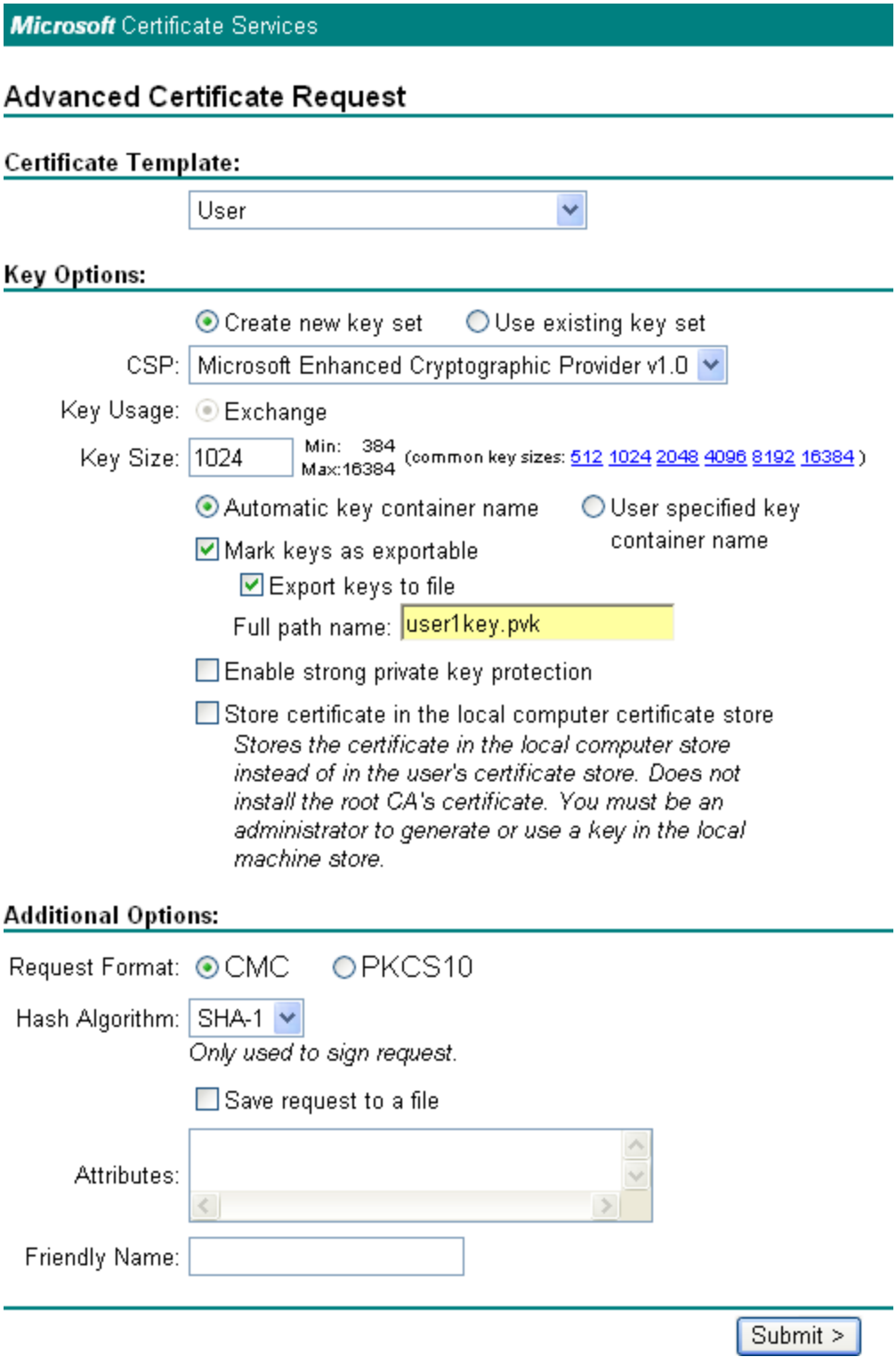
Request a Certificate Screen

Click on the **advanced certificate request** link.



Advanced Certificate Request Screen

Click on the **Create and submit a request to this CA** link.



Advanced Certificate Details

For the **Certificate Template**, select **User**.

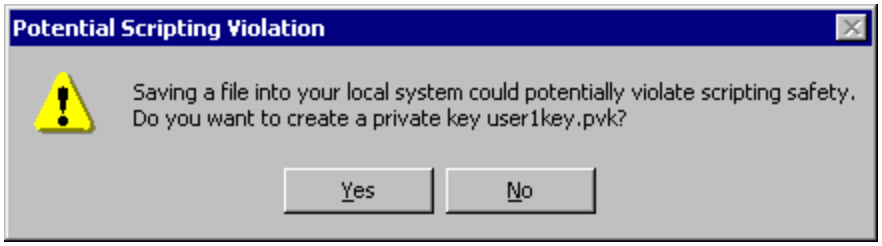
Check the **Mark keys as exportable** and the **Export keys to file** checkboxes.

Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

Be sure to note the name used for the private key file, for example LXEUSER.PVK. The certificate file created later in this process must be given the same name, for example, LXEUSER.CER.

DO NOT check to use strong private key protection.

Make any other desired changes and click the **Submit** button.



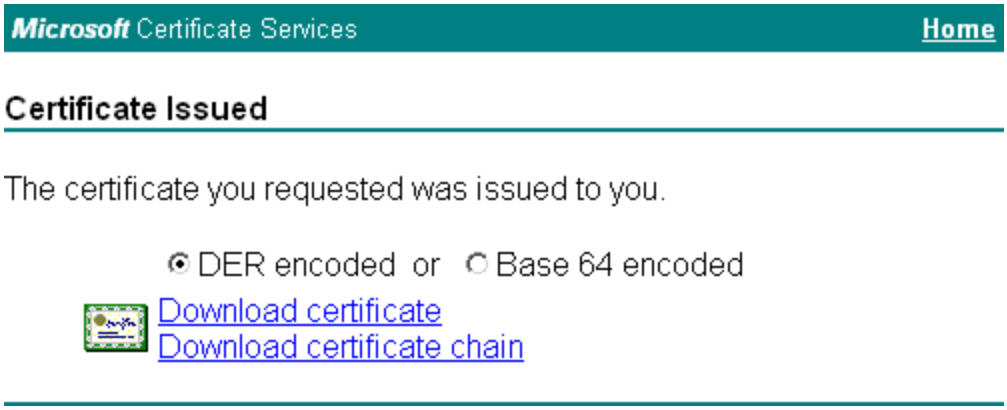
Script Warnings

If any script notifications occur, click the "**Yes** button to continue the certificate request.

Private Key Password

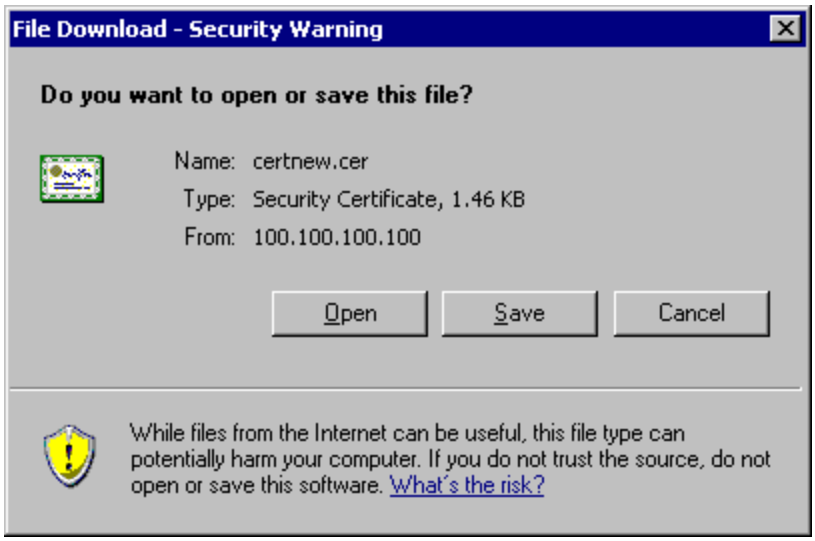
When prompted for the private key password:

- Click **None** if you do not wish to use a password, or
- Enter and confirm your desired password then click **OK**.



Certificate Issued

Click the **Download certificate** link.



Download Security Warning

Click **Save** to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.

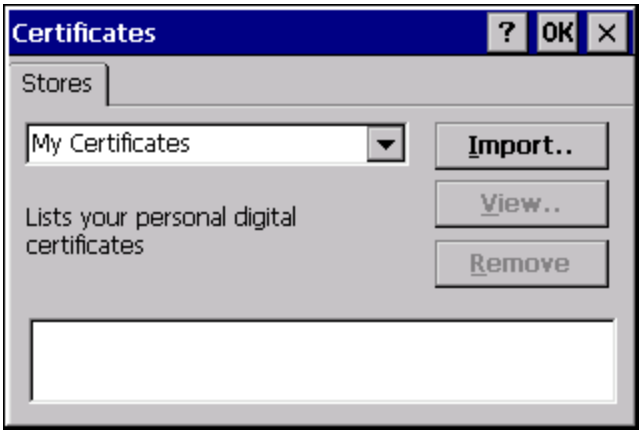
Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as LXEUSER.PVK then the certificate file created must be given the same name, for example, LXEUSER.CER.

Install the user certificate.

Installing a User Certificate

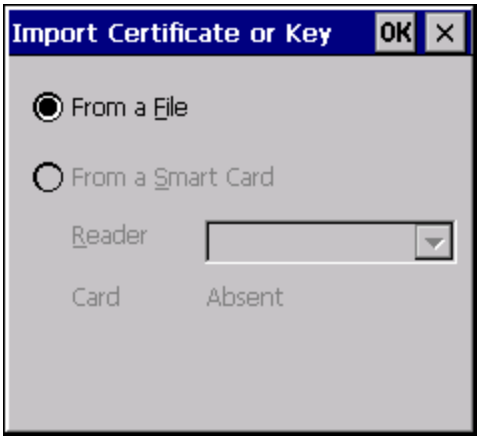
Copy the certificate and private key files to the HX2. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Select **My Certificates** from the pull down list.



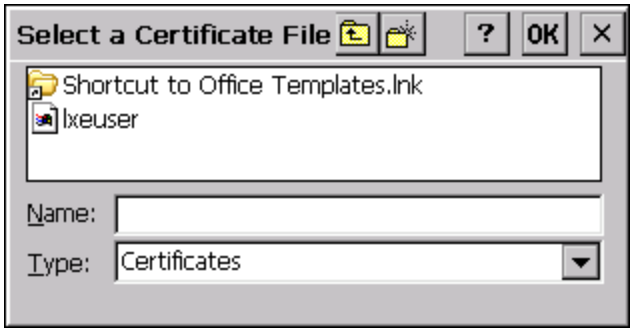
Certificates

Tap the **Import** button.



Import Certificate

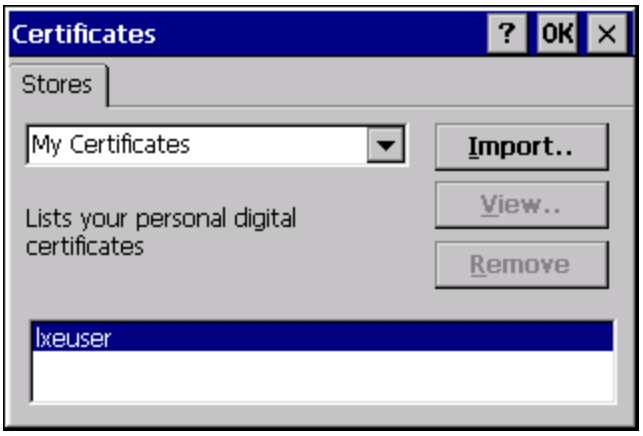
Make sure **From a File** is selected and tap **OK**.



Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.

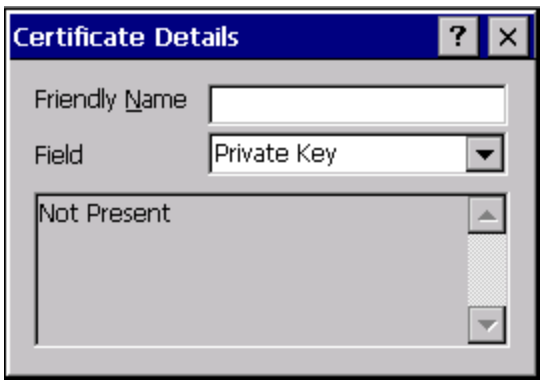
The certificate is now shown in the list.



Certificate Listing

With the certificate you just imported highlighted, tap **View**.

From the Field pull down menu, select **Private Key**.

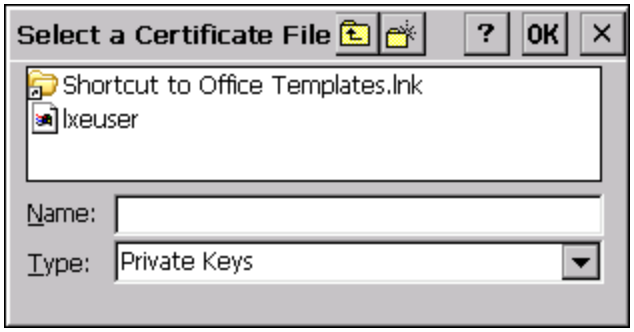


Private Key Not Present

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap **OK** to return to the Certificates screen.

Tap import.



Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to **Private Keys**, select the certificate desired and tap **OK**. Enter the password for the certificate if appropriate.

Verify Installation

Tap on **View** to see the certificate details again.

Private Key Present

The private key should now say present. If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example LXEuser.cer for the certificate and LXEuser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

Keymaps

Alpha Mode 3 Tap	The HX2 default keypad on all HX2s shipped prior to September 2007. Setup requires no user interaction.
Dual Alpha	Set as the default keypad when the Dual Alpha or Triple Tap keypad has been shipped.
Triple Tap	Requires file activation to setup the Triple Tap keypad for daily use. Setup requires the Use Triple Tap Keypad checkbox be checked in the HX2 Options Control Panel. Tap OK.

Alpha Mode 3 Tap

Hints

- When using a sequence of keys that require an alpha key, first press the Alpha key.
- Double tap the Alpha key for upper case alphabetic characters.
- Single tap the Alpha key to enter and exit Alpha mode.
- Default Alpha mode produces lower case alphabetic characters when numeric keys are pressed.
- Pressing the Alpha key forces “Alpha” mode for all keys.
- To create a combination of numbers and letters before pressing Enter, remember to tap the Alpha key to toggle between Alpha and Numeric mode.
- Use the Input Panel to enter characters that are not available using the 23-key keypad.
- When using a sequence of keys that do not include the Alpha key (Orange) but does include a sticky key (Blue), press the Blue key first then the rest of the key sequence.

To get this Key / Function	Press these Keys in this Order	
Power / Suspend	Power	
Volume Up	Blue	Up Arrow
Volume Down	Blue	Down Arrow
Blue Mode (Toggle)	Blue	
Alpha Mode (Toggle)	Alpha	
Diamond Key	Blue	Enter
Start Button	Only available when Mapped	
Display Brightness Increase / Decrease	Only available when	

To get this Key / Function	Press these Keys in this Order	
	Mapped	
Uppercase Alpha (Toggle)	Alpha	Doubleclick (similar to CapsLock. Single tap the Alpha key to exit CapsLock mode)
Lowercase Alpha	This is the default	
Space	Alpha	0
Enter	Enter	
CapsLock Mode	Alpha (times 2)	Alpha
Back Space	Backspace	
Escape	Blue	Backspace
Tab	Blue	Right Arrow
Back Tab	Blue	Left Arrow
Up Arrow (Cursor Up)	Up Arrow	
Down Arrow (Cursor Down)	Down Arrow	
Right Arrow (Cursor Right)	Right Arrow	
Left Arrow (Cursor Left)	Left Arrow	
F1	F1	
F2	F2	
F3	F3	
F4	F4	
F5	Blue	F1
F6	Blue	F2
F7	Blue	F3
F8	Blue	F4
F9	Only available when Mapped	
F10	Blue	0
F11	Blue	1
F12	Blue	2
F13	Blue	3
F14	Blue	4
F15	Blue	5
F16	Blue	6
F17	Blue	7
F18	Blue	8
F19	Blue	9

To get this Key / Function	Press these Keys in this Order	
F20 through F24	Only available when Mapped	
a	Alpha	2
b	Alpha	22
c	Alpha	222
d	Alpha	3
e	Alpha	33
f	Alpha	333
g	Alpha	4
h	Alpha	44
i	Alpha	444
j	Alpha	5
k	Alpha	55
l	Alpha	555
m	Alpha	6
n	Alpha	66
o	Alpha	666
p	Alpha	7
q	Alpha	77
r	Alpha	777
s	Alpha	7777
t	Alpha	8
u	Alpha	88
v	Alpha	888
w	Alpha	9
x	Alpha	99
y	Alpha	999
z	Alpha	9999
A	Alpha (times 2)	2
B	Alpha (times 2)	22
C	Alpha (times 2)	222
D	Alpha (times 2)	3
E	Alpha (times 2)	33
F	Alpha (times 2)	333

To get this Key / Function	Press these Keys in this Order	
G	Alpha (times 2)	4
H	Alpha (times 2)	44
I	Alpha (times 2)	444
J	Alpha (times 2)	5
K	Alpha (times 2)	55
L	Alpha (times 2)	555
M	Alpha (times 2)	6
N	Alpha (times 2)	66
O	Alpha (times 2)	666
P	Alpha (times 2)	7
Q	Alpha (times 2)	77
R	Alpha (times 2)	777
S	Alpha (times 2)	7777
T	Alpha (times 2)	8
U	Alpha (times 2)	88
V	Alpha (times 2)	888
W	Alpha (times 2)	9
X	Alpha (times 2)	99
Y	Alpha (times 2)	999
Z	Alpha (times 2)	9999
1	1 and 11111 (Alpha Mode)	
2	2 and 2222 (Alpha Mode)	
3	3 and 3333 (Alpha Mode)	
4	4 and 4444 (Alpha Mode)	
5	5 and 5555 (Alpha Mode)	
6	6 and 6666 (Alpha Mode)	
7	7 and 77777 (Alpha Mode)	
8	8 and 8888 (Alpha Mode)	

To get this Key / Function	Press these Keys in this Order	
9	9 and 99999 (Alpha Mode)	
0	0 and 00 (Alpha Mode)	
. (period)	Alpha	1
/	Alpha	11
* (asterisk)	Alpha	111
- (dash or minus sign)	Alpha	1111

Special Keys

Dual Alpha

Hints

- Any key press exits out of the volume and backlight control modes.
- Modifier keys are sticky.
- A modifier key (Green, Orange, Blue, Shift and Control) pressed after itself toggles that modifier key off.
- Any key other than a modifier key following any modifier key, unsticks the modifier keys.

To get this Key / Function	Press these Keys in this Order			
Power / Suspend	Power / Suspend			
Volume Up	Orange	Diamond 1	Up Arrow	
Volume Down	Orange	Diamond 1	Down Arrow	
Display Backlight Increase	Blue	Diamond 1	Up Arrow	
Display Backlight Decrease	Blue	Diamond 1	Down Arrow	
Alt Mode	Green	Ctrl		
Ctrl Mode	Ctrl			
Escape	ESC			
Green Mode (Toggle)	Green	Green		
Orange Mode (Toggle)	Orange	Orange		
Blue Mode (Toggle)	Blue	Blue		
Diamond 1 Mode	Diamond 1			
Diamond 2 Mode	Green	Diamond 1		
Start Button	Ctrl	Esc		
Uppercase Alpha (Toggle)	Shift			
Lowercase Alpha (default setting)				
Space	Green	BKSP (Backspace)		
Enter	Enter			
Capslock (Toggle)	Not applicable			
Back Space	Backspace			

To get this Key / Function	Press these Keys in this Order			
Tab	Tab			
BackTab	Green	Tab		
Up Arrow (Cursor Up)	Up Arrow			
Down Arrow (Cursor Down)	Down Arrow			
Right Arrow (Cursor Right)	Green	Down Arrow		
Left Arrow (Cursor Left)	Green	Up Arrow		
Insert	Orange	Blue	5	
Delete	Orange	Blue	1	
Home	Orange	Blue	7	
End	Orange	Blue	3	
Page Up	Orange	Blue	0	
Page Down	Orange	Blue	BKSP (Backspace)	
F1	Green	1		
F2	Green	2		
F3	Green	3		
F4	Green	4		
F5	Green	5		
F6	Green	6		
F7	Green	7		
F8	Green	8		
F9	Green	9		
F10	Green	0		
F11	Green	Shift	1	
F12	Green	Shift	2	
F13	Green	Shift	3	
F14	Green	Shift	4	
F15	Green	Shift	5	
F16	Green	Shift	6	
F17	Green	Shift	7	
F18	Green	Shift	8	
F19	Green	Shift	9	
F20	Green	Shift	0	
F21	Green	Blue	Shift	1
F22	Green	Blue	Shift	2

To get this Key / Function	Press these Keys in this Order			
F23	Green	Blue	Shift	3
F24	Green	Blue	Shift	4
a	Orange	1		
b	Blue	1		
c	Orange	2		
d	Blue	2		
e	Orange	3		
f	Blue	3		
g	Orange	4		
h	Blue	4		
i	Orange	5		
j	Blue	5		
k	Orange	6		
l	Blue	6		
m	Orange	7		
n	Blue	7		
o	Orange	8		
p	Blue	8		
q	Orange	9		
r	Blue	9		
s	Orange	Up Arrow		
t	Blue	Up Arrow		
u	Orange	0		
v	Blue	0		
w	Orange	BKSP		
x	Blue	BKSP		
y	Orange	Down Arrow		
z	Blue	Down Arrow		
A	Orange	Shift	1	
B	Blue	Shift	1	
C	Orange	Shift	2	
D	Blue	Shift	2	
E	Orange	Shift	3	
F	Blue	Shift	3	

To get this Key / Function	Press these Keys in this Order			
G	Orange	Shift	4	
H	Blue	Shift	4	
I	Orange	Shift	5	
J	Blue	Shift	5	
K	Orange	Shift	6	
L	Blue	Shift	6	
M	Orange	Shift	7	
N	Blue	Shift	7	
O	Orange	Shift	8	
P	Blue	Shift	8	
Q	Orange	Shift	9	
R	Blue	Shift	9	
S	Orange	Shift	Up Arrow	
T	Blue	Shift	Up Arrow	
U	Orange	Shift	0	
V	Blue	Shift	0	
W	Orange	Shift	BKSP	
X	Blue	Shift	BKSP	
Y	Orange	Shift	Down Arrow	
Z	Blue	Shift	Down Arrow	
1	1			
2	2			
3	3			
4	4			
5	5			
6	6			
7	7			
8	8			
9	9			
0	0			
. (period)	Orange	Tab		
* (asterisk)	Blue	Tab		
- (dash or minus sign)	Green	Blue	Tab	
/	Green	Blue	0	

To get this Key / Function	Press these Keys in this Order			
‘ (single quote)	Green	Blue	1	
[	Green	Blue	2	
]	Green	Blue	3	
\	Green	Blue	4	
‘ (apostrophe)	Green	Blue	5	
, (comma)	Green	Blue	6	
` (accent)	Green	Blue	7	
; (semicolon)	Green	Blue	8	
= (equal sign)	Green	Blue	9	
!	Shift	1		
@	Shift	2		
#	Shift	3		
$	Shift	4		
%	Shift	5		
^	Shift	6		
&	Shift	7		
* (asterisk)	Shift	8		
(	Shift	9		
)	Shift	0		
“ (double quote)	Green	Orange	1	
{	Green	Orange	2	
}	Green	Orange	3	
| (broken bar)	Green	Orange	4	
~ (tilde)	Green	Orange	5	
<	Green	Orange	6	
>	Green	Orange	7	
: (colon)	Green	Orange	8	
+ (plus sign)	Green	Orange	9	
?	Green	Orange	0	
_ (underscore)	Green	Orange	TAB	

Triple Tap

Hints

- Any key press exits out of the volume and backlight control modes.
- Modifier keys are sticky.
- A modifier key (Green, Orange, Blue, Shift and Control) pressed after itself toggles that modifier key off.
- Any key other than a modifier key following any modifier key, unsticks the modifier keys.

To get this Key / Function	Press these Keys in this Order			
Power / Suspend	Power / Suspend			
Volume Up	Orange	Diamond 1	Up Arrow	
Volume Down	Orange	Diamond 1	Down Arrow	
Display Backlight Increase	Blue	Diamond 1	Up Arrow	
Display Backlight Decrease	Blue	Diamond 1	Down Arrow	
Alt Mode	Green	Ctrl		
Ctrl Mode	Ctrl			
Escape	ESC			
Green Mode (Toggle)	Green	Green		
Orange Mode (Toggle)	Orange	Orange		
Blue Mode (Toggle)	Blue	Blue		
Diamond 1 Mode	Diamond 1			
Diamond 2 Mode	Green	Diamond 1		
Start Button	Ctrl	Esc		
Uppercase Alpha (Toggle)	Shift			
Lowercase Alpha (default setting)				
Space	Green	BKSP (Backspace)		
Enter	Enter			
Capslock (Toggle)	Not applicable			

To get this Key / Function	Press these Keys in this Order			
Back Space	Backspace			
Tab	Tab			
BackTab	Green	Tab		
Up Arrow (Cursor Up)	Up Arrow			
Down Arrow (Cursor Down)	Down Arrow			
Right Arrow (Cursor Right)	Green	Down Arrow		
Left Arrow (Cursor Left)	Green	Up Arrow		
Insert	Orange	Blue	5	
Delete	Orange	Blue	1	
Home	Orange	Blue	7	
End	Orange	Blue	3	
Page Up	Orange	Blue	0	
Page Down	Orange	Blue	BKSP (Backspace)	
F1	Green	1		
F2	Green	2		
F3	Green	3		
F4	Green	4		
F5	Green	5		
F6	Green	6		
F7	Green	7		
F8	Green	8		
F9	Green	9		
F10	Green	0		
F11	Green	Shift	1	
F12	Green	Shift	2	
F13	Green	Shift	3	
F14	Green	Shift	4	
F15	Green	Shift	5	
F16	Green	Shift	6	
F17	Green	Shift	7	
F18	Green	Shift	8	
F19	Green	Shift	9	
F20	Green	Shift	0	
F21	Green	Blue	Shift	1

To get this Key / Function	Press these Keys in this Order			
F22	Green	Blue	Shift	2
F23	Green	Blue	Shift	3
F24	Green	Blue	Shift	4
a	Blue	2		
b	Blue	22		
c	Blue	222		
d	Blue	3		
e	Blue	33		
f	Blue	333		
g	Blue	4		
h	Blue	44		
i	Blue	444		
j	Blue	5		
k	Blue	55		
l	Blue	555		
m	Blue	6		
n	Blue	66		
o	Blue	666		
p	Blue	7		
q	Blue	77		
r	Blue	777		
s	Blue	7777		
t	Blue	8		
u	Blue	88		
v	Blue	888		
w	Blue	9		
x	Blue	99		
y	Blue	999		
z	Blue	9999		
A	Blue	Shift	2	
B	Blue	Shift	22	
C	Blue	Shift	222	
D	Blue	Shift	3	
E	Blue	Shift	33	

To get this Key / Function	Press these Keys in this Order			
F	Blue	Shift	333	
G	Blue	Shift	4	
H	Blue	Shift	44	
I	Blue	Shift	444	
J	Blue	Shift	5	
K	Blue	Shift	55	
L	Blue	Shift	555	
M	Blue	Shift	6	
N	Blue	Shift	66	
O	Blue	Shift	666	
P	Blue	Shift	7	
Q	Blue	Shift	77	
R	Blue	Shift	777	
S	Blue	Shift	7777	
T	Blue	Shift	8	
U	Blue	Shift	88	
V	Blue	Shift	888	
W	Blue	Shift	9	
X	Blue	Shift	99	
Y	Blue	Shift	999	
Z	Blue	Shift	9999	
1	1			
2	2	or 2222		
3	3	or 3333		
4	4	or 4444		
5	5	or 5555		
6	6	or 6666		
7	7	or 77777		
8	8	or 8888		
9	9	or 99999		
0	0			
. (period)	Orange	Tab		
* (asterisk)	Blue	Tab		
- (dash or minus sign)	Green	Blue	Tab	

To get this Key / Function	Press these Keys in this Order			
/	Green	Blue	0	
‘ (single quote)	Green	Blue	1	
[	Green	Blue	2	
]	Green	Blue	3	
\	Green	Blue	4	
‘ (apostrophe)	Green	Blue	5	
, (comma)	Green	Blue	6	
` (accent)	Green	Blue	7	
; (semicolon)	Green	Blue	8	
= (equal sign)	Green	Blue	9	
!	Shift	1		
@	Shift	2		
#	Shift	3		
$	Shift	4		
%	Shift	5		
^	Shift	6		
&	Shift	7		
* (asterisk)	Shift	8		
(	Shift	9		
)	Shift	0		
“ (double quote)	Green	Orange	1	
{	Green	Orange	2	
}	Green	Orange	3	
| (broken bar)	Green	Orange	4	
~ (tilde)	Green	Orange	5	
<	Green	Orange	6	
>	Green	Orange	7	
: (colon)	Green	Orange	8	
+ (plus sign)	Green	Orange	9	
?	Green	Orange	0	
_ (underscore)	Green	Orange	TAB	

Technical Specifications

Processor	Intel Xscale operating at 400 MHz
Memory	128MB SDRAM / 128MB flash
Mass Storage	SD Card - SD/MMC 1-bit interface
Operating System	Microsoft® Windows® CE 5
Radio Modules	802.11 a/b/g radio / Bluetooth
Scanner options	No scanner | SE955 standard range laser | SE4400 2D imager
Display technology	QVGA Transflective Color / LED backlight. 320 horizontal x 240 vertical pixels. One Quarter VGA portrait. 2.5 (6.3cm) diagonal viewing area. Color scale is TFT display color depth of 64K. Active area 1.47" x 1.97" (3.7 cm x 5 cm).
Main Battery, Standard	Li-Ion battery pack 7.2V. Tethered. Voltage range 6.0-8.4VDC.
Main Battery, Extended	Li-Ion battery pack 7.2V. Tethered. Voltage range 6.0-8.4VDC.
Backup Battery	CMOS Internal Nickel Cadmium (NiCd) 4.8V / 1.2V nominal. Automatically charges from main battery during normal operation. Memory operational for 24 hours when main battery is depleted.
Audio/Microphone Connector	Tethered Cable: Audio/Battery/HX2 Cable
External I/O Ports	Serial Port (COM2) (2) Tethered cable Ring scanner. Max baud rate 230.4Kbps. Main Battery | Cradle Connection (COM1) Asynchronous port. Max baud rate 230.4Kbps. | Bluetooth Connection (COM3) Max baud rate 921.6Kbps.

Dimensions and Weight

Dimension	
Length	3.50 in | 8.89 cm
Width	4.98 in | 12.55 cm
Height	1.40 in | 3.56 cm
Weight	
HX2 with network card, standard battery and ring scanner	1 lb 0.5 oz 462 g
Battery Standard	4.1 oz | 116 g
Battery Extended	7.2 oz | 205 g
Ring Scanner	1.7 oz | 48 g
Ring Imager	1.8 oz | 51 g

Environmental Specifications

Operating Temperature	-4°F to 122°F (-20°C to 50°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
ESD	8 KV air, 4kV direct contact
Operating Humidity	5% to 90% non-condensing
Water and Dust	IEC 60529 compliant to IP54
Vibration	Based on MIL Std 810D

Network Card Specifications

Summit 802.11 b/g CF 2.4GHz

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	50 mW max.
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	Same as HX2 Operating Temperature
Storage Temperature	Same as HX2 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Summit 802.11a/b/g CF 2.4/5.0GHz

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.0GHz IEEE 802.11a DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	FCC: 1-11, 36, 40 ,44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44 ,48
Operating Temperature	Same as HX2 Operating Temperature
Storage Temperature	Same as HX2 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Bluetooth

Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No more than 32.80 feet (10 meters) line of sight
Bluetooth Version	2.0 + EDR

AppLock Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_ PROCESSING
App= <Application name>	Name of the application being locked	LOG_ PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
**********	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_ PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete	LOG_ERROR

Message	Explanation and/or corrective action	Level
	AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key	Unable to encrypt password.	LOG_ERROR

Message	Explanation and/or corrective action	Level
failure		
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_ PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_ PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_ PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_ PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_ PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_ PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_ PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_ PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_ PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_ PROCESSING
Enter verify password	Entering the password verification processing.	LOG_ PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_ PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_ PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Exit EncryptPwd	Exiting password encryption processing.	LOG_ PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_ PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_ PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_ PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_ PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_ PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_ PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_ PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_ PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_ PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_ PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_ PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_ PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_ PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_ PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_ PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_ PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_ PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_ WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_ PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_ PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_ PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_ PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_ PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_ PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_ PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_ PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_ PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_ PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_ PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX

Message	Explanation and/or corrective action	Level
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Ù	DB	~[
Ú	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

Revision History

Revision / Date	Location / Change
M / Sep 2011	1. Bluetooth. / Options added: can connect to up to four Bluetooth devices, HID/PAN/DUN. can send / receive files using Object Push Profile (OPP). 2. Operating System. / Revised *Folders Copied at Startup*. Replaced and revised *Reflash* with *Upgrade the Operating System*. 3. Summit Client Utility. / Roam Delta default changed to 5 dBm. Added new parameter: WAPI, default is Off (dimmed). 4. Technical Specifications / Updated Channel list for a/b/g radio.
L / Jan 2011	1. Links added. Images updated. Clarified instructions. 2. Added 1GB or less SD flash card statement to Reflash instruction.
K / May 2010	1. Introduction / Added Reboot instruction. 2. Bluetooth. / Added Filtered Mode to Control Panel. 3. Wireless Network Configuration. / Added new global parameters, revised encryption option names to match screen displays, updated radio mode and profile parameters.
J / Mar 2010	1. Introduction. / Added EULA instruction. Added Continuous Scan Mode caution. 2. ActiveSync. / Updated ActiveSync Troubleshooting. 3. Control Panel. / Added Device Management, Installed Programs, Network Capture. Revised Mixer Output. 4. Control Panel, Scanner. / Added Continuous Scan Mode. Revised Scanner Main Tab. 5. Technical Specifications. / Revised Environmental Specifications.
H / Dec 2009	AppLock Troubleshooting. / Removed back door code for AppLock.
G / Oct 2009	1. Cover page and contents. / Applied Marketing color scheme. 2. Introduction. / Removed "Features". 3. Avalanche Enabler. / Changed HX2_Enabler_CAB to LXE_Enabler_CAB. 4. Scanner Wedge. / Added reset instruction when resetting rings to factory default settings.
F / Aug 2009 F / Dec 2008	F / Aug 2009 / Formatted for browser delivery. F / Dec 2008 - : Chapter 1 – Introduction-Added “Toggle the Status Popup Window On or Off”. Chapter 3 – System Configuration-Added “Status Popup Tab” to HX2-3 Options. Chapter 5 – Wireless Network Configuration-Added note: “IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes. If changes are made to the stored credentials, click Commit to save those changes first before making any additional changes.”. Entire Manual-Add new armband and cable pictures where applicable.
E / Oct 2008	Chapter 5 – Wireless Network Configuration - Added sections: “Auto Profile” and “Auth Server”. Revised sections: “Main Tab”, “Radio Mode” and “Hide Password”. Appendix A – KeyMaps - Corrected forward slash and backslash keypress sequences for the Alpha Mode 3 Tap keypad.

D / Sep 2008	Chapter 1 – Introduction-Updated graphics. Updated Connecting the Battery and Ring Scanner.Removed references to Creating Custom Key Maps. Added Continuous Scan Mode. Removed Copy the HX2 LXEbook to the HX2. Chapter 3 – System Configuration-Added HX2-3 Options control panel. Updated Keypad Control Panel. Updated Scanner | Barcode tab panel to add Continuous Scan. Removed Pocket Inbox, Word Viewer, PDF Viewer, Excel Viewer, Image Viewer, Media Player, VOIP Demo. Removed Configuring GrabTime, Configuring CapsLock Behavior. Chapter 5 – Wireless Network Configuration-Revised section Summit Client Configuration. Chapter 4 – Scanner-Updated Barcode Processing Overview. Added Continuous Scan Mode. Chapter 6 – AppLock-Added AppLock Options Panel. Added AppLock Match.
C / May 2008	Chapter 1 – Introduction - Revised “Setup the Client and Network”. Updated “Accessories”. Chapter 3 – System Configuration - Revised “Control Panel Options” to add “WiFi”. Upgraded Enabler to 4.2. Added “eXpress Scan”. Added “LXE Connect.” Chapter 5 – Wireless Network Configuration - Revised the following sections: “Introduction”, “Summit Radio”, “Summit Client Utility”, “Main Tab”. Revised Profile Tab parameter: “Radio Mode”. Revised Global Tab parameters: “TX Diversity”, “Rx Diversity”. Added Global Mode parameter: “DFS Channels”. • Appendix B – Technical Specifications - Revised “Network Device Specifications”.
B / Nov 2007	Chapter 1 – Introduction - Updated Strap Assemblies. Replaced Using the 23 Key Keypad with HX2 Keypads. Added Adjusting the Display Brightness. Added Ring Scanner Strap Kit, Trigger Assembly 20 pack, and Bluetooth Mobile Barcode Readers to Accessories. Chapter 2 – Physical Description and Layout - Updated Cradle LED indicator segment. Chapter 3 – System Configuration - Updated Wavelink Avalanche naming conventions in Wavelink Avalanche Enabler and Wavelink Avalanche Enabler Configuration. Updated Keypad section to include keypad control panel options for three keypad configurations. Updated GrabTime section. Updated Bluetooth sections. Chapter 4 – Scanner - Added Length Based Barcode Stripping instruction. Chapter 5 – Wireless Network Configuration - Added EAP-TLS instruction. Updated Summit Client Utility to reflect version differences. Chapter 6 – AppLock - Added keypress instructions for the Alpha Mode 3 Tap (the original), Dual Alpha and Triple Tap keypads. Appendix A – Key Maps - Added Alpha Mode 3 Tap Keypad, Dual Alpha Keypad and Triple Tap Keypad keymaps. Added Display Brightness to Alpha Mode 3 Tap keypad. Appendix B – Technical Specifications - Updated HX2 physical dimensions. Entire Guide - Added keyed instructions for the Alpha Mode 3 Tap (the original keypad), Dual Alpha and Triple Tap keypads where applicable. Updated LXEZ Pairing and Bluetooth instruction where applicable.
A / May 2007	Initial Release.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W